

53-1001775-01  
13 April 2010



# DCFM Enterprise

---

## User Manual

**Supporting DCFM 10.4.X**

**BROCADE**

Copyright © 2007-2010 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, IronPoint, IronShield, IronView, IronWare, JetCore, NetIron, SecureIron, ServerIron, StorageX, and Turbolron are registered trademarks, and DCFM, Extraordinary Networks, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

## Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters  
Brocade Communications Systems, Inc.  
1745 Technology Drive  
San Jose, CA 95110  
Tel: 1-408-333-8000  
Fax: 1-408-333-8101  
E-mail: [info@brocade.com](mailto:info@brocade.com)

European Headquarters  
Brocade Communications Switzerland Sàrl  
Centre Swissair  
Tour B - 4ème étage  
29, Route de l'Aéroport  
Case Postale 105  
CH-1215 Genève 15  
Switzerland  
Tel: +41 22 799 5640  
Fax: +41 22 799 5641  
E-mail: [emea-info@brocade.com](mailto:emea-info@brocade.com)

Asia-Pacific Headquarters  
Brocade Communications Systems China HK, Ltd.  
No. 1 Guanghua Road  
Chao Yang District  
Units 2718 and 2818  
Beijing 100020, China  
Tel: +8610 6588 8888  
Fax: +8610 6588 9999  
E-mail: [china-info@brocade.com](mailto:china-info@brocade.com)

Asia-Pacific Headquarters  
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)  
Citic Plaza  
No. 233 Tian He Road North  
Unit 1308 – 13th Floor  
Guangzhou, China  
Tel: +8620 3891 2000  
Fax: +8620 3891 2111  
E-mail: [china-info@brocade.com](mailto:china-info@brocade.com)

## Document History

The following table lists all versions of the DCFM Enterprise User Manual.

Document Title	Publication Number	Summary of Changes	Publication Date
DCFMEnterprise User Manual	53-1001072-01	First release	August 2008
DCFMEnterprise User Manual	53-1001196-01	Updated for 10.1.X release.	December 2008
DCFMEnterprise User Manual	53-1001260-01	Updated for 10.2.X release.	April 2009
DCFMEnterprise User Manual	53-1001357-01	Updated for 10.3.X release.	July 2009
DCFMEnterprise User Manual	53-1001775-01	Updated for 10.4.X release.	April 2010

# Contents

---

## About This Document

In this chapter .....	xxvii
How this document is organized .....	xxvii
Supported hardware and software .....	xxviii
Supported open source software products .....	xxxi
What's new in this document .....	xxxii
Document conventions .....	xxxiv
Text formatting .....	xxxiv
Notes, cautions, and warnings .....	xxxiv
Key terms .....	xxxiv
Notice to the reader .....	xxxv
Additional information .....	xxxv
Brocade resources .....	xxxv
Other industry resources .....	xxxvi
Getting technical help .....	xxxvi
Document feedback .....	xxxvii

## Chapter 1

### Getting Started

In this chapter .....	1
User interface components .....	1
Menu bar .....	3
Toolbar .....	3
SAN tab .....	4
View All list .....	4
Port Display buttons .....	5
Product List .....	5
Connectivity Map .....	6
Toolbox .....	7
Master Log .....	7
Utilization Legend .....	8
Minimap .....	9
Status bar .....	10
Icon legend .....	11
Product icons .....	11
Group icons .....	12
Port icons .....	12
Product status icons .....	13
Event icons .....	13

Management server and client .....	14
Logging into a server .....	17
Launching a remote client .....	17
Clearing previous versions of the remote client .....	18
Launching the Configuration Wizard .....	18
Changing your password .....	22
Changing the database user password .....	22
Viewing active sessions .....	23
Disconnecting users .....	23
Viewing server properties .....	24
Viewing port status .....	24
License .....	25
Managed port count calculation .....	25
Entering the license key .....	26
Upgrading the application .....	26
Installing a patch .....	27
Uninstalling a patch .....	28
Feature-to-firmware requirements .....	29
Accessibility features for the Management application .....	31
Keyboard shortcuts .....	31
Look and Feel .....	32

## Chapter 2

### Discovery

In this chapter .....	35
Fabric discovery overview .....	35
FCS policy and seed switches .....	36
Discovering fabrics .....	36
Configuring SNMP credentials .....	39
Reverting to a default SNMP community string .....	41
Deleting a fabric .....	41
Host discovery .....	42
Discovering Hosts by IP address or hostname .....	42
Importing Hosts from a CSV file .....	43
Importing Hosts from a Fabric .....	44
Configuring Brocade HBA credentials .....	45
Configuring virtual machine credentials .....	46
Editing Host credentials .....	47
Removing a Host from Discovery .....	48
Viewing the discovery state .....	48
Troubleshooting discovery .....	49
M-EOSn discovery troubleshooting .....	50
Virtual Fabric discovery troubleshooting .....	51
Fabric monitoring .....	52
Monitoring discovered fabrics .....	52
Stop monitoring of a discovered fabric .....	53

Seed switch . . . . .	53
Seed switch requirements. . . . .	54
Seed switch failover. . . . .	55
Changing the seed switch . . . . .	56
 <b>Chapter 3</b>	
<b>Application Configuration</b>	
In this chapter . . . . .	59
Data backup . . . . .	59
What is backed up? . . . . .	59
Management server backup . . . . .	60
Configuring backup to a writable CD . . . . .	61
Configuring backup to a hard drive. . . . .	62
Configuring backup to a network drive. . . . .	63
Enabling backup. . . . .	64
Disabling backup . . . . .	64
Viewing the backup status . . . . .	65
Changing the backup interval . . . . .	65
Starting immediate backup. . . . .	66
Reviewing backup events . . . . .	66
Data restore. . . . .	67
Restoring data . . . . .	67
Restoring data to a new server. . . . .	68
Display . . . . .	68
Setting your FICON display . . . . .	68
Resetting your display . . . . .	69
End node display. . . . .	70
Displaying end nodes. . . . .	70
Ethernet events. . . . .	71
Enabling Ethernet events . . . . .	71
Disabling Ethernet events . . . . .	72
Event storage. . . . .	72
Configuring event storage . . . . .	72
Flyovers . . . . .	73
Configuring flyovers . . . . .	73
Turning flyovers on or off. . . . .	76
Viewing flyovers . . . . .	76
Names . . . . .	76
Setting names to be unique . . . . .	76
Setting names to be non-unique. . . . .	77
Fixing duplicate names . . . . .	78
Viewing names. . . . .	79
Adding a name to an existing device . . . . .	79
Adding a name to a new device . . . . .	80
Applying a name to a detached WWN . . . . .	80
Removing a name from a device . . . . .	80

Editing names .....	81
Exporting names .....	81
Importing Names .....	82
Searching for a device by name .....	82
Searching for a device by WWN .....	83
Security .....	84
Configuring the server name .....	84
Setting the CHAP secret .....	85
Configuring login security .....	85
Configuring the login banner display .....	86
Disabling the login banner .....	86
Software Configuration .....	87
Client export port .....	87
Discovery .....	88
FTP/SCP overview .....	89
IP Configuration .....	93
Memory allocation .....	97
Server port .....	100
Support mode .....	101
Fabric tracking .....	102
Enabling fabric tracking .....	103
Disabling fabric tracking .....	103
Accepting changes for a fabric .....	104
Accepting changes for a device .....	104

## Chapter 4

### Call Home

In this chapter .....	105
About call home .....	106
System requirements .....	107
Showing a call home center .....	108
Hiding a call home center .....	109
Editing a call home center .....	109
Editing the Brocade International or IBM call home center ..	109
Editing the Brocade North America call home center .....	111
Editing an E-mail call home center .....	112
Editing the EMC call home center .....	113
Editing the HP LAN call home center .....	114
Enabling a call home center .....	115
Enabling support save .....	115
Testing the call home center connection .....	116
Disabling a call home center .....	116
Viewing Call Home status .....	117
Assigning a device to the call home center .....	118
Removing a device from a call home center .....	118
Removing all devices and filters from a call home center .....	119

Defining an event filter .....	119
Call Home for virtual switches .....	119
Assigning an event filter to a call home center .....	120
Assigning an event filter to a device .....	120
Overwriting an assigned event filter .....	121
Removing an event filter from a call home center .....	121
Removing an event filter from a device .....	122
Removing an event filter from the Call Home Event Filters table .....	122
Searching for an assigned Event Filter .....	122

## Chapter 5

### View management

In this chapter .....	123
About view management .....	123
Creating a customized view .....	124
Editing a customized view .....	125
Deleting a customized view .....	126
Copying a view .....	127
About topology layout .....	127
Customizing the layout of devices on the topology .....	128
Customizing the layout of connections on the topology .....	129
Changing a group's background color .....	129
Reverting to the default background color .....	130
Changing the product label .....	131
Changing the port label .....	131
Changing the port display .....	131
Grouping on the topology .....	132
Collapsing groups .....	132
Expanding groups .....	132
Viewing connections .....	132
Configuring custom connections .....	132
Saving a custom connection configuration .....	133
Deleting a custom connection configuration .....	133
Customizing the main window .....	134
Zooming in and out of the connectivity map .....	134
Showing levels of detail on the connectivity map .....	135
Exporting the topology .....	135
Customizing application tables .....	136
Searching for a device in the connectivity map .....	139

<b>Chapter 6</b>	<b>Third-party tools</b>
	In this chapter .....141
	About third-party tools .....141
	Starting third-party tools from the application .....142
	Launching a Telnet session .....142
	Launching an Element Manager .....143
	Launching Web Tools .....143
	Launching FCR configuration .....144
	Launching HCM Agent .....145
	Adding a tool .....146
	Entering the server IP address of a tool .....147
	Adding an option to the Tools menu .....147
	Changing an option on the Tools menu .....149
	Removing an option from the Tools menu .....149
	Adding an option to a device's shortcut menu .....150
	Changing an option on a device's shortcut menu .....151
	Removing an option from a device's shortcut menu .....152
	VMware vCenter plug-in .....153
	Registering a vCenter server .....153
	Editing a vCenter server .....154
	Deleting a vCenter server .....154
<b>Chapter 7</b>	<b>Server Management Console</b>
	In this chapter .....155
	Server management console overview .....155
	Launching the SMC on Windows .....155
	Launching the SMC on Linux and Solaris .....156
	Services .....156
	Monitoring and managing Management application services .....156
	Refreshing the server status .....157
	Stopping all services .....157
	Stopping the CIMOM services .....157
	Starting all services .....158
	Restarting all services .....158
	Changing server port numbers .....158
	Authentication .....159
	Configuring a Radius server .....159
	Configuring an LDAP server .....161
	Configuring switch authentication .....162
	Configuring Windows authentication .....163

Configuring NIS authentication . . . . .	164
Configuring UNIX password file authentication . . . . .	164
Configuring local database authentication . . . . .	164
Displaying the client authentication audit trail . . . . .	165
Restoring the database . . . . .	165
Capturing technical support information . . . . .	167
Upgrading HCM on the Management server . . . . .	168
SMI Agent configuration . . . . .	169
Launching the SMIA configuration tool on Windows . . . . .	169
Launching the SMIA configuration tool on Linux and Solaris . . . . .	170
Launching a remote SMIA configuration tool . . . . .	171
Home tab . . . . .	171
Authentication . . . . .	172
CIMOM configuration . . . . .	175
Certificate management . . . . .	177
Viewing the configuration summary . . . . .	180

## Chapter 8

### Device Configuration

In this chapter . . . . .	183
Configuration repository management . . . . .	183
Saving switch configurations . . . . .	184
Restoring a switch configuration for a selected device . . . . .	185
Backing up a switch configuration . . . . .	186
Restoring a configuration from the repository . . . . .	188
Viewing configuration file content . . . . .	189
Searching the configuration file content . . . . .	190
Deleting a configuration . . . . .	190
Exporting a configuration . . . . .	191
Importing a configuration . . . . .	191
Keeping a copy past the defined age limit . . . . .	191
Replicating configurations . . . . .	191
Replicating security configurations . . . . .	192
Device properties . . . . .	192
Viewing properties . . . . .	192
Adding a property label . . . . .	195
Editing a property label . . . . .	195
Deleting a property label . . . . .	196
Editing a property field . . . . .	196
Enhanced group management . . . . .	196
Firmware management . . . . .	197
Displaying the firmware repository . . . . .	197
Importing a firmware file and release notes . . . . .	198
Deleting a firmware file . . . . .	199
Download firmware . . . . .	199

Host port mapping .....	201
Creating a new Host. ....	201
Renaming an HBA Host .....	202
Deleting an HBA Host .....	202
Viewing Host properties. ....	202
Associating an HBA with a Host .....	203
Importing HBA-to-Host mapping .....	203
Removing an HBA from a Host .....	204
Exporting Host port mapping .....	205
Ports .....	206
Viewing port connectivity. ....	206
Refreshing the port connectivity view. ....	209
Enabling a port. ....	209
Disabling a port .....	209
Filtering port connectivity .....	210
Viewing port details .....	211
Viewing ports and port properties .....	212
Port types .....	215
Showing connected ports .....	215
Viewing port connection properties .....	216
Determining inactive iSCSI devices .....	218
Determining port status .....	218
Viewing port optics. ....	219
Port Auto Disable. ....	221
Viewing the port auto disable status .....	221
Enabling port auto disable on individual ports .....	222
Enabling port auto disable on all ports on a device .....	222
Disabling port auto disable on individual ports. ....	223
Disabling port auto disable on all ports on a device. ....	223
Unblocking ports .....	223
Storage port mapping configuration .....	224
Creating a storage array .....	224
Adding storage ports to a storage array .....	225
Unassigning a storage port from a storage array .....	225
Reassigning mapped storage ports .....	225
Editing storage array properties .....	226
Deleting a storage array .....	226
Viewing storage port properties .....	227
Viewing storage array properties .....	227
Importing storage port mapping. ....	228
Exporting storage port mapping .....	229
Device Technical Support .....	230
Scheduling technical support information collection .....	230
Starting immediate technical support information collection .....	231
Viewing technical support information. ....	232
E-mailing technical support information .....	232
Copying technical support information to an external FTP server. ....	233
Deleting technical support files from the repository. ....	233

	Upload Failure data capture . . . . .	234
	Enabling upload failure data capture . . . . .	234
	Disabling upload failure data capture . . . . .	235
	Purging upload failure data capture files . . . . .	235
	Configuring the upload failure data capture FTP server . . . .	236
	Viewing the upload failure data capture repository . . . . .	237
<b>Chapter 9</b>	<b>Fabric Binding</b>	
	In this chapter . . . . .	239
	Fabric binding overview . . . . .	239
	Enabling fabric binding . . . . .	240
	Disabling fabric binding . . . . .	241
	Adding switches to the fabric binding membership list . . . .	241
	Adding detached devices to the fabric binding membership list . . . . .	242
	Removing switches from fabric binding membership . . . . .	242
	High integrity fabrics . . . . .	243
	High integrity fabric requirements . . . . .	244
	Activating high integrity fabrics . . . . .	244
	Deactivating high integrity fabrics . . . . .	245
<b>Chapter 10</b>	<b>Fault Management</b>	
	In this chapter . . . . .	247
	Fault management overview . . . . .	247
	Event logs . . . . .	248
	Viewing event logs . . . . .	248
	Copying part of a log entry . . . . .	249
	Copying an entire log entry . . . . .	249
	Exporting the entire log . . . . .	250
	E-mailing all event details from the Master Log . . . . .	250
	E-mailing selected event details from the Master Log . . . .	250
	E-mailing a range of event details from the Master Log . . . .	251
	Displaying event details from the Master Log . . . . .	251
	Copying part of the Master Log . . . . .	252
	Copying the entire Master Log . . . . .	252
	Exporting the Master Log . . . . .	253
	Filtering events in the Master Log . . . . .	253
	Setting up advanced event filtering for the Master Log . . . .	254
	Removing an advanced event filter . . . . .	256
	Event policies . . . . .	257
	Policy types . . . . .	257
	Policy triggers . . . . .	258
	Policy actions . . . . .	258
	Adding an event policy . . . . .	258
	Adding an Port offline policy . . . . .	259
	Adding a PM threshold crossed policy . . . . .	260
	Adding a security violation policy . . . . .	261

Defining the broadcast message action . . . . .	262
Defining the launch script action . . . . .	263
Defining the send e-mail action . . . . .	264
Configuring support data capture action . . . . .	265
Activating a policy . . . . .	265
Deactivating a policy . . . . .	265
Deleting a policy . . . . .	266
Duplicating an event policy . . . . .	266
Duplicating an Port offline policy . . . . .	267
Duplicating a PM threshold crossed policy . . . . .	268
Duplicating a security violation policy . . . . .	269
Editing an event policy . . . . .	270
Editing an Port offline policy . . . . .	271
Editing a PM threshold crossed policy . . . . .	272
Editing a security violation policy . . . . .	273
Viewing events . . . . .	273
Event notification . . . . .	274
Configuring e-mail notification . . . . .	274
Setting up advanced event filtering for a user . . . . .	275
SNMP trap and informs registration and forwarding . . . . .	278
Registering the management server . . . . .	278
Registering a different Management application server . . . . .	278
Removing a host server . . . . .	279
Enabling trap forwarding . . . . .	279
Adding an SNMPv1 destination . . . . .	279
Adding an SNMPv3 destination . . . . .	280
Editing a destination . . . . .	281
Removing a destination . . . . .	281
Disabling trap forwarding . . . . .	281
Enabling SNMP informs . . . . .	282
Disabling SNMP informs . . . . .	282
Syslog forwarding . . . . .	283
Registering the management server . . . . .	283
Registering a host server . . . . .	284
Removing a host server . . . . .	284
Adding a destination . . . . .	284
Editing a destination . . . . .	285
Removing a destination . . . . .	285
Enabling Syslog forwarding . . . . .	285
Disabling Syslog forwarding . . . . .	286

## Chapter 11

### Performance Data

In this chapter . . . . .	287
Performance overview . . . . .	287
Performance measures . . . . .	288
Performance management requirements . . . . .	289
Real-time performance data . . . . .	293
Generating a real-time performance graph . . . . .	294
Filtering real-time performance data . . . . .	295

Exporting real-time performance data .....	296
Clearing port counters .....	296
Historical performance data .....	297
Enabling historical performance collection SAN wide .....	297
Enabling historical performance collection for selected fabrics .....	297
Disabling historical performance collection .....	298
Generating a historical performance graph .....	298
Saving a historical performance graph configuration .....	300
Exporting historical performance data .....	301
Deleting a historical performance graph .....	301
End-to-end monitoring .....	302
Configuring an end-to-end monitor pair .....	302
Displaying end-to-end monitor pairs in a real-time graph ...	303
Displaying end-to-end monitor pairs in a historical graph ...	303
Refreshing end-to-end monitor pairs .....	304
Deleting an end-to-end monitor pair .....	304
Top Talker monitoring .....	304
Configuring a fabric mode Top Talker monitor .....	305
Configuring an F_port mode Top Talker monitor .....	307
Deleting a Top Talker monitor .....	308
Pausing a Top Talker monitor .....	308
Restarting a Top Talker monitor .....	308
Thresholds and event notification .....	309
Creating a threshold policy .....	309
Editing a threshold policy .....	311
Duplicating a threshold policy .....	313
Assigning a threshold policy .....	313
Deleting a threshold policy .....	314
Connection utilization .....	315
Enabling connection utilization .....	316
Disabling connection utilization .....	316
Changing connection utilization .....	317

## Chapter 12

### Reports

In this chapter .....	319
Report types .....	319
Generating reports .....	320
Viewing reports .....	320
Exporting reports .....	321
Printing reports .....	322
Deleting reports .....	322
Generating performance reports .....	323
Generating zoning reports .....	324

## Chapter 13

### Port Fencing

In this chapter .....	325
About port fencing .....	325
Port Fencing requirements .....	325
Thresholds .....	326
C3 Discard Frames threshold .....	326
Invalid CRCs threshold .....	327
Invalid words threshold .....	327
Link threshold .....	327
Link Reset threshold .....	327
Protocol error threshold .....	328
State Change threshold .....	328
Security threshold .....	328
Adding thresholds .....	329
Adding a C3 Discard Frames threshold .....	329
Adding an Invalid CRCs threshold .....	331
Adding an Invalid Words threshold .....	332
Adding a Link threshold .....	333
Adding a Link Reset threshold .....	334
Adding a Protocol Error threshold .....	335
Adding a State Change threshold .....	336
Adding a Security threshold .....	338
Assigning thresholds .....	339
Unblocking a port .....	339
Avoiding port fencing inheritance .....	340
Editing thresholds .....	340
Editing a C3 Discard Frames threshold .....	340
Editing an Invalid CRCs threshold .....	341
Editing an Invalid Words threshold .....	342
Editing a Link threshold .....	343
Editing a Link Reset threshold .....	344
Editing a Protocol Error threshold .....	345
Editing a State Change threshold .....	346
Editing a Security threshold .....	347
Finding assigned thresholds .....	348
Viewing thresholds .....	348
Viewing all thresholds on a specific device .....	349
Removing thresholds .....	349
Removing thresholds from individual objects .....	349
Removing thresholds from the thresholds table .....	350

## Chapter 14

### Role-Based Access Control

In this chapter .....	351
Users .....	351
Viewing the list of users .....	351
Adding a user account .....	352
Editing a user account .....	353
Filtering event notifications for a user .....	353
Removing a user account .....	354

Roles .....	355
Creating a user role .....	355
Editing a user role .....	356
Removing a user role .....	357
Resource groups .....	358
Creating a resource group .....	358
Editing a resource group .....	359
Removing a resource group .....	360
Assigning a user to a resource group .....	361
Removing a user from a resource group .....	362
Finding a user's resource group .....	362

## Chapter 15

### Host management

In this chapter .....	363
About host management .....	363
HCM software .....	364
HCM features .....	364
Host bus adapters .....	365
Converged network adapters .....	366
Host discovery .....	367
Connectivity map .....	367
View management .....	368
Host port mapping .....	368
Role-based access control .....	369
Host management privileges .....	369
Host administrator privileges .....	369
Host performance management .....	370
Host fault management .....	371
Adapter events .....	371
Event policies .....	371
Filtering event notifications .....	372
Syslog forwarding .....	372
Host security authentication .....	373
Configuring security authentication using the Management application .....	373
supportSave on adapters .....	374

## Chapter 16

### Fibre Channel over IP

In this chapter .....	375
FCIP services licensing .....	376
FCIP Concepts .....	376
IP network considerations .....	376
FCIP platforms and supported features .....	377

FCIP trunking . . . . .	379
Design for redundancy and fault tolerance . . . . .	379
FCIP tunnel restrictions for FCP and FICON emulation features. . . . .	379
FCIP Trunk configuration considerations . . . . .	380
FCIP circuit failover capabilities . . . . .	380
Bandwidth calculation during failover . . . . .	381
Adaptive Rate Limiting . . . . .	382
FSPF link cost calculation when ARL is used. . . . .	382
QoS SID/DID priorities over an FCIP trunk . . . . .	383
IPsec and IKE implementation over FCIP . . . . .	384
IPsec for the 4 Gbps platforms . . . . .	384
IPSec for the 8 Gbps platforms. . . . .	385
QoS, DSCP, and VLANs . . . . .	386
DSCP quality of service . . . . .	386
VLANs and layer two quality of service. . . . .	386
When both DSCP and L2CoS are used. . . . .	387
Open systems tape pipelining . . . . .	388
FCIP Fastwrite and Tape Acceleration . . . . .	388
FICON emulation features . . . . .	389
XRC emulation . . . . .	389
Tape write pipelining . . . . .	389
Tape read pipelining . . . . .	389
FCIP configuration guidelines. . . . .	390
Virtual Port Types . . . . .	390
Configuring an FCIP tunnel. . . . .	391
Adding an FCIP circuit. . . . .	393
Configuring FCIP tunnel advanced settings . . . . .	396
Enabling and disabling compression . . . . .	396
Enabling Open Systems Tape Pipelining (OSTP) . . . . .	397
Enabling Tperf test mode . . . . .	397
Configuring IPsec and IKE policies. . . . .	398
Configuring FICON emulation . . . . .	399
Viewing FCIP connection properties . . . . .	401
Viewing General FCIP properties . . . . .	402
Viewing FCIP FC port properties. . . . .	403
Viewing FCIP Ethernet port properties. . . . .	404
Editing FCIP tunnels . . . . .	405
Editing FCIP circuits . . . . .	406
Disabling FCIP tunnels . . . . .	407
Enabling FCIP tunnels. . . . .	407
Deleting FCIP tunnels . . . . .	408
Disabling FCIP circuits . . . . .	408

Enabling FCIP circuits .....	408
Deleting FCIP Circuits .....	408
Displaying FCIP performance graphs.....	409
Displaying performance graphs for FC ports .....	409
Displaying FCIP performance graphs for Ethernet ports....	409
Displaying tunnel properties from the FCIP tunnels dialog box...	410
Displaying FCIP circuit properties from the FCIP tunnels dialog box. ....	411
Displaying switch properties from the FCIP Tunnels dialog box...	412
Displaying fabric properties from the FCIP Tunnels dialog box...	413
Troubleshooting FCIP Ethernet connections .....	414

## Chapter 17

### Fibre Channel over Ethernet

In this chapter .....	415
FCoE overview .....	415
DCB exchange protocol .....	415
Enhanced Ethernet features .....	416
Enhanced transmission selection.....	416
Priority-based flow control.....	416
Ethernet jumbo frames .....	416
FCoE protocols supported .....	417
Ethernet link layer protocols supported .....	417
FCoE protocols .....	417
FCoE Licensing .....	418
Save running to startup .....	418
Copying switch configurations to selected switches .....	418
CEE configuration .....	419
Opening the CEE Configuration dialog box.....	420
CEE configuration tasks .....	421
Minimum CEE configuration for FCoE traffic .....	422
Switch policies.....	426
CEE map and Traffic Class map .....	426
LLDP profiles .....	426
Access control lists .....	426
Spanning Tree Protocol policy .....	427
802.1x policy .....	427
Link aggregation groups.....	427
Adding a LAG .....	427
Editing a CEE switch .....	430
Editing a CEE port .....	431
Editing a LAG .....	432
Enabling a CEE port or LAG.....	434
Deleting a LAG .....	434

CEE Performance .....	435
Real Time Performance Graph .....	435
Historical Performance Graph .....	436
Historical Performance Report .....	436
QoS configuration .....	437
Enhanced Transmission Selection .....	437
Priority-based flow control .....	437
Creating a CEE map .....	438
Editing a CEE map .....	439
Deleting a CEE map .....	440
Assigning a CEE map to a port or link aggregation group ...	441
Creating a traffic class map .....	442
Editing a traffic class map .....	442
Deleting a traffic class map .....	443
Assigning a traffic class map to a port or link aggregation group .....	443
LLDP-DCBX configuration .....	445
Configuring LLDP for FCoE .....	445
Adding an LLDP profile .....	446
Editing an LLDP profile .....	447
Deleting an LLDP profile .....	447
Assigning an LLDP profile to a port or ports in a LAG .....	448
Access Control List configuration .....	450
Adding an ACL to a switch .....	450
Editing the parameters of an ACL .....	452
Deleting an ACL .....	453
Assigning an ACL to a port or link aggregation group .....	453
Spanning Tree Protocol configuration .....	455
Enabling Spanning Tree Protocol .....	455
Setting Spanning Tree parameters for a switch .....	456
STP configurable parameters at the port or LAG level .....	459
802.1x authentication .....	460
Enabling 802.1x authentication .....	460
Disabling 802.1x .....	461
Setting 802.1x parameters for a switch .....	461
CEE switch management using Web Tools .....	463
CEE switch management using Telnet .....	464
Virtual FCoE port configuration .....	464
Viewing virtual FCoE ports .....	465
Clearing a stale entry .....	466

## Chapter 18

### FICON Environments

In this chapter .....	467
FICON Configurations .....	467
Configuring a PDCM Allow/Prohibit Matrix .....	468
Configuring an Allow/Prohibit manually .....	470

	Saving or Copying a PDCM configuration to another device . . . . .	471
	Copying a PDCM configuration . . . . .	471
	Saving a PDCM configuration to another device . . . . .	473
	Activating a PDCM configuration . . . . .	474
	Deleting a PDCM configuration . . . . .	475
	Changing the PDCM matrix display . . . . .	475
	Cascaded FICON fabric . . . . .	476
	Configuring a cascaded FICON fabric . . . . .	477
	Cascaded FICON fabric merge . . . . .	479
	Merging two cascaded FICON fabrics . . . . .	480
	Resolving merge conflicts . . . . .	482
	Port Groups . . . . .	483
	Creating a port group . . . . .	483
	Viewing port groups . . . . .	484
	Editing a port group . . . . .	485
	Deleting a port group . . . . .	485
	Swapping blades . . . . .	486
<b>Chapter 19</b>	<b>FC-FC Routing Service Management</b>	
	In this chapter . . . . .	487
	Devices that support Fibre Channel routing . . . . .	487
	Fibre Channel routing overview . . . . .	488
	Guidelines for setting up FC-FC routing . . . . .	489
	Connecting edge fabrics to a backbone fabric . . . . .	490
	Configuring routing domain IDs . . . . .	492
<b>Chapter 20</b>	<b>Encryption configuration</b>	
	In this chapter . . . . .	493
	Encryption Center features . . . . .	494
	Encryption user privileges . . . . .	495
	Smart card usage . . . . .	496
	Registering authentication cards from a card reader . . . . .	496
	Registering authentication cards from the database . . . . .	497
	De-registering an authentication card . . . . .	498
	Using authentication cards . . . . .	498
	Enabling or disabling the system card requirement . . . . .	499
	Registering system cards from a card reader . . . . .	499
	De-registering a system card . . . . .	500
	Tracking smart cards . . . . .	500
	Editing smart cards . . . . .	501
	Network connections . . . . .	502
	Configuring blade processor links . . . . .	502
	Encryption node initialization and certificate generation . . . . .	503

Supported encryption key manager appliances .....	504
Steps for connecting to an RKM appliance .....	504
Exporting the KAC certificate signing request (CSR) .....	505
Submitting the CSR to a certificate authority .....	505
Importing the signed KAC certificate .....	505
Uploading the KAC and CA certificates onto the RKM appliance .....	506
RKM key vault high availability deployment .....	507
Steps for connecting to an LKM appliance .....	507
The NetApp DataFort Management Console .....	508
Establishing the trusted link .....	508
Obtaining and importing the LKM certificate .....	509
Exporting and registering the switch KAC certificates on LKM .....	510
LKM key vault high availability deployment .....	510
Disk keys and tape pool keys (Brocade native mode support) .....	510
Tape LUN and DF-compatible tape pool support .....	511
LKM Key Vault Deregistration .....	511
Steps for connecting to an SKM appliance .....	511
Configuring a Brocade group on SKM .....	512
Registering the SKM Brocade group user name and password .....	513
Setting up the local Certificate Authority (CA) on SKM .....	514
Downloading the local CA certificate from SKM .....	515
Creating and installing the SKM server certificate .....	515
Enabling SSL on the Key Management System (KMS) Server .....	516
Creating an SKM High Availability cluster .....	517
Copying the local CA certificate for a clustered SKM appliance .....	517
Adding SKM appliances to the cluster .....	518
Signing the Brocade encryption node KAC certificates .....	519
Importing a signed KAC certificate into a switch .....	519
Steps for connecting to a TEMS appliance .....	520
Setting up TEMS network connections .....	520
Creating a client on TEMS .....	521
Establishing TEMS key vault credentials on the switch .....	522
Gathering information .....	523
Creating a new encryption group .....	524
Adding a switch to an encryption group .....	536
Replacing an encryption engine in an encryption group .....	540
Creating high availability (HA) clusters .....	541
Removing engines from an HA cluster .....	542
Swapping engines in an HA cluster .....	543
Failback option .....	543
Invoking failback .....	543
Adding encryption targets .....	544
Configuring hosts for encryption targets .....	551

Adding target disk LUNs for encryption . . . . .	552
Remote replication LUNs . . . . .	554
SRDF pairs . . . . .	554
Metadata requirements and remote replication . . . . .	555
Adding Target Tape LUNs for encryption . . . . .	556
Configuring encrypted tape storage in a multi-path environment . . . . .	557
Re-balancing the encryption engine . . . . .	558
Master keys . . . . .	559
Active master key . . . . .	559
Alternate master key . . . . .	559
Master key actions . . . . .	560
Reasons master keys can be disabled . . . . .	560
Saving the master key to a file . . . . .	560
Saving a master key to a key vault . . . . .	562
Saving a master key to a smart card set . . . . .	563
Restoring a master key from a file . . . . .	565
Restoring a master key from a key vault . . . . .	566
Restoring a master key from a smart card set . . . . .	567
Creating a new master key . . . . .	568
Zeroizing an encryption engine . . . . .	569
Encryption Targets dialog box . . . . .	570
Redirection zones . . . . .	572
Disk device decommissioning . . . . .	573
Decommissioning LUNs . . . . .	573
Displaying and deleting decommissioned key IDs . . . . .	574
Viewing and editing switch encryption properties . . . . .	574
Exporting the public key certificate signing request (CSR) from Properties . . . . .	577
Importing a signed public key certificate from Properties . . . . .	577
Enabling the encryption engine state from Properties . . . . .	578
Disabling the encryption engine state from Properties . . . . .	578
Viewing and editing group properties . . . . .	578
General tab . . . . .	579
Members tab . . . . .	580
Consequences of removing an encryption switch . . . . .	581
Security tab . . . . .	583
HA Clusters tab . . . . .	584
Engine Operations tab . . . . .	584
Link Keys tab . . . . .	585
Tape Pools tab . . . . .	585
Encryption-related acronyms in log messages . . . . .	587

## Chapter 21

### Virtual Fabrics

In this chapter .....	589
Virtual Fabrics overview .....	589
Terminology .....	590
Virtual Fabrics requirements .....	590
Configuring Virtual Fabrics .....	592
Enabling Virtual Fabrics on a discovered device .....	593
Disabling Virtual Fabrics on a discovered device .....	593
Creating a logical switch or base switch .....	593
Finding the physical chassis for a logical switch .....	595
Finding the logical switch from a physical chassis .....	596
Assigning ports to a logical switch .....	596
Removing ports from a logical switch .....	597
Deleting a logical switch .....	598
Configuring fabric-wide parameters for a logical fabric. ....	598
Applying logical fabric settings to all associated logical switches	599
Moving a logical switch to a different fabric. ....	600
Changing a logical switch to a base switch .....	601

## Chapter 22

### Zoning

In this chapter .....	603
Zoning overview. ....	603
Types of zones .....	603
Online zoning .....	604
Offline zoning .....	604
Accessing zoning .....	605
Zoning naming conventions .....	605
Administrator zoning privileges .....	605
Zoning configuration. ....	607
Configuring zoning for the SAN .....	607
Creating a new zone .....	608
Viewing zone properties .....	609
Adding members to a zone .....	609
Creating a new member in a zone by WWN .....	610
Creating a new member in a zone by domain, port index. ...	612
Creating a new member in a zone by alias .....	613
Enabling or disabling the default zone for fabrics .....	614
Enabling or disabling safe zoning mode for fabrics .....	615
Creating a zone alias .....	615
Editing a zone alias .....	616
Removing an object from a zone alias .....	617
Exporting zone aliases .....	617
Renaming a zone alias .....	617
Creating a zone configuration .....	618
Viewing zone configuration properties .....	618

Adding zones to a zone configuration .....	619
Activating a zone configuration .....	620
Deactivating a zone configuration .....	622
Creating an offline zone database .....	623
Refreshing a zone database .....	624
Merging two zone databases .....	624
Saving a zone database to a switch .....	626
Exporting an offline zone database .....	627
Importing an offline zone database .....	627
Rolling back changes to the offline zone database .....	627
LSAN zoning .....	628
Configuring LSAN zoning .....	628
Creating a new LSAN zone .....	629
Adding members to the LSAN zone .....	629
Creating a new member in an LSAN zone .....	630
Activating LSAN zones .....	631
Traffic isolation zoning .....	632
Enhanced TI zones .....	632
Configuring traffic isolation zoning .....	633
Creating a traffic isolation zone .....	634
Adding members to a traffic isolation zone .....	635
Enabling a traffic isolation zone .....	636
Disabling a traffic isolation zone .....	636
Enabling failover on a traffic isolation zone .....	637
Disabling failover on a traffic isolation zone .....	637
Zoning administration .....	638
Comparing zone databases .....	638
Managing zone configuration comparison alerts .....	640
Setting change limits on zoning activation .....	640
Deleting a zone .....	641
Deleting a zone alias .....	641
Deleting a zone configuration .....	642
Deleting an offline zone database .....	642
Clearing the fabric zone database .....	643
Removing all user names from a zone database .....	643
Duplicating a zone .....	644
Duplicating a zone alias .....	645
Duplicating a zone configuration .....	645
Finding a member in one or more zones .....	646
Finding a zone member in the potential member list .....	646
Finding zones in a zone configuration .....	647
Finding a zone configuration member in the zones list .....	647
Listing zone members .....	648
Removing a member from a zone .....	648
Removing a zone from a zone configuration .....	649
Removing an offline device .....	649
Renaming a zone .....	650
Renaming a zone configuration .....	650
Replacing zone members .....	651
Replacing an offline device by WWN .....	652
Replacing an offline device by name .....	653

<b>Chapter 23</b>	<b>Troubleshooting</b>
	In this chapter .....655
	FC troubleshooting .....655
	Tracing FC routes ..... 656
	Troubleshooting device connectivity..... 657
	Confirming fabric device sharing ..... 658
	IP troubleshooting.....659
	Configuring IP ping..... 659
	Tracing IP routes..... 661
	Viewing FCIP tunnel performance..... 662
	Client browser troubleshooting .....663
	Fabric tracking troubleshooting.....663
	FICON troubleshooting .....664
	Firmware download troubleshooting.....664
	Launch Client troubleshooting.....665
	Names troubleshooting .....667
	Performance troubleshooting.....667
	Port Fencing troubleshooting.....671
	Server Management Console troubleshooting.....672
	Supportsave troubleshooting.....673
	View All list troubleshooting .....674
	Zoning troubleshooting.....674
<b>Appendix A</b>	<b>Application menus</b>
	In this appendix.....675
	Main menus.....675
	Shortcut menus.....682
<b>Appendix B</b>	<b>Call Home Event Tables</b>
	In this appendix.....695
	Call Home Event Table .....695
	# CONSRV Events Table .....697
	# Thermal Event Reason Codes Table.....697
	# Brocade Events Table .....698
<b>Appendix C</b>	<b>User Privileges</b>
	In this appendix.....699
	About User Privileges .....699
	About Roles and Access Levels ..... 717

**Appendix D****Sybase and Derby Database Fields**

In this appendix . . . . .	719
Database tables and fields . . . . .	720
Advanced Call Home . . . . .	720
Capability . . . . .	721
Client_view . . . . .	722
Collector . . . . .	725
Config . . . . .	728
Connected end devices . . . . .	730
Device . . . . .	731
EE- Monitor . . . . .	738
Event/FM . . . . .	740
Fabric . . . . .	746
FC Port Stats . . . . .	749
FCIP . . . . .	752
FCIP Tunnel Stats . . . . .	755
GigE Port Stats . . . . .	757
ISL . . . . .	759
License . . . . .	762
Encryption Device . . . . .	763
Encryption Container . . . . .	769
Meta SAN . . . . .	774
Network . . . . .	776
Others . . . . .	777
Port Fencing . . . . .	778
Quartz . . . . .	779
Reports . . . . .	782
Role Based Access Control . . . . .	782
SNMP . . . . .	785
Stats . . . . .	788
Switch . . . . .	790
Switch details . . . . .	795
Switch port . . . . .	800
Switch SNMP info . . . . .	805
Threshold . . . . .	807
User Interface . . . . .	808
Zoning 1 . . . . .	809
Zoning 2 . . . . .	811

**Index**



# About This Document

---

## In this chapter

- [How this document is organized](#) . . . . . xxvii
- [Supported hardware and software](#). . . . . xxviii
- [Supported open source software products](#) . . . . . xxxi
- [What's new in this document](#) . . . . . xxxii
- [Document conventions](#) . . . . . xxxiv
- [Additional information](#). . . . . xxxv
- [Getting technical help](#) . . . . . xxxvi
- [Document feedback](#) . . . . . xxxvii

## How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible. This document supports DCFM 10.4.0 and later.

The document contains the following components:

- [Chapter 1, “Getting Started,”](#) provides a high-level overview of the user interface.
- [Chapter 2, “Discovery,”](#) describes how to discover SANs and hosts.
- [Chapter 3, “Application Configuration,”](#) provides Management application configuration instructions.
- [Chapter 4, “Call Home,”](#) provides call home configuration instructions.
- [Chapter 5, “View management,”](#) provides view and topology configuration instructions.
- [Chapter 6, “Third-party tools,”](#) provides instructions for adding and launching third-party tools.
- [Chapter 7, “Server Management Console,”](#) provides information on using the Server Management Console to stop and start the Management application services, back up the Management application database, and capture technical support information.
- [Chapter 8, “Device Configuration,”](#) provides device configuration instructions.
- [Chapter 9, “Fabric Binding,”](#) provides fabric binding instructions.
- [Chapter 10, “Fault Management,”](#) provides event management instructions.
- [Chapter 11, “Performance Data,”](#) provides information on how to manage performance.
- [Chapter 12, “Reports,”](#) provides instructions for generating reports.
- [Chapter 13, “Port Fencing,”](#) provides information on how to configure port fencing.
- [Chapter 14, “Role-Based Access Control,”](#) provides information on how to manage users.

- [Chapter 15, “Host management,”](#) provides information on how to configure an HBA.
- [Chapter 16, “Fibre Channel over IP,”](#) provides information on how to configure an FCIP.
- [Chapter 17, “Fibre Channel over Ethernet,”](#) provides information on how to configure an FCoE.
- [Chapter 18, “FICON Environments,”](#) provides information on how to manage FICON.
- [Chapter 19, “FC-FC Routing Service Management,”](#) provides information on how to manage Fibre Channel Routing.
- [Chapter 20, “Encryption configuration,”](#) provides information on configuring encryption.
- [Chapter 21, “Virtual Fabrics,”](#) provides information on configuring and managing logical switches.
- [Chapter 22, “Zoning,”](#) provides zoning configuration instructions.
- [Chapter 23, “Troubleshooting,”](#) provides troubleshooting details.
- [Appendix A, “Application menus,”](#) provides information about the main and shortcut menus.
- [Appendix B, “Call Home Event Tables,”](#) provides supplemental information about call home event tables.
- [Appendix C, “User Privileges,”](#) provides supplemental information about user privileges and access levels.
- [Appendix D, “Sybase and Derby Database Fields,”](#) provides reference information related to databases.

## Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for DCFM 10.4.X, documenting all possible configurations and scenarios is beyond the scope of this document.

The following firmware platforms are supported by this release of DCFM 10.4.X:

- Fabric OS 5.0 or later in a pure Fabric OS fabric
- Fabric OS 6.0 or later in a Mixed Fabric

For platform specific Fabric OS requirements, refer to the [Table 1](#) footnotes.

---

**NOTE**

Discovery of a Secure Fabric OS fabric in strict mode is not supported.

---

- M-EOS and M-EOSn 9.6.X or later in a mixed Fabric OS and M-EOS fabric
- M-EOS and M-EOSn 9.9.2 or later in a pure M-EOS fabric

The hardware platforms in the following table are supported by this release of DCFM 10.4.X.

**TABLE 1** Supported Hardware

Device Name	Terminology used in documentation
Brocade 200E switch	16-port, 4 Gbps FC Switch
Brocade 300 switch <sup>6</sup>	24-port, 8 Gbps FC Switch
Brocade 4012 switch	Embedded 12-port, 4 Gbps FC Switch
Brocade 4016 switch	Embedded 16-port, 4 Gbps FC Switch
Brocade 4018 switch	Embedded 18-port, 4 Gbps FC Switch
Brocade 4020 switch	Embedded 20-port, 4 Gbps FC Switch
Brocade 4024 switch <sup>5</sup>	Embedded 24-port, 4 Gbps FC Switch
Brocade 4100 switch	32-port, 4 Gbps FC Switch
Brocade 4900 switch <sup>2</sup>	64-port, 4 Gbps FC Switch
Brocade 5000 switch <sup>3</sup>	32-port, 4 Gbps FC Interop Switch
Brocade 5100 switch <sup>6</sup>	40-port, 8 Gbps FC Switch
Brocade 5300 switch <sup>6</sup>	80-port, 8 Gbps FC Switch
Brocade 5410 embedded switch <sup>6</sup>	8 Gbps 12-port Embedded Switch
Brocade M5424 embedded switch	8 Gbps 24-port Embedded Switch
Brocade 5450 embedded switch	8 Gbps 16-port Embedded Switch
Brocade 5460 embedded switch	8 Gbps 24-port Embedded Switch
Brocade 5470 embedded switch	8 Gbps 24-port Embedded Switch
Brocade 5480 embedded switch <sup>6</sup>	8 Gbps 24-port Embedded Switch
Brocade 7500 Extension switch <sup>1</sup>	4 Gbps Router, Extension Switch
Brocade 7500E Extension switch <sup>1</sup>	4 Gbps Extension Switch
FR4-18i Blade	4 Gbps Router, Extension blades
Brocade AP7600 switch <sup>6</sup>	4 Gbps 32-port Switch
Brocade 7800 Switch <sup>11</sup>	8 Gbps 16-FC ports, 6-Gbit ports Extension Switch
Brocade 8000 switch <sup>10</sup>	24 - 8 Gbps FC Port, 8 - 10 Gbps CEE Port Switch
Brocade 8470 FCoE embedded switch <sup>12</sup>	FCoE Embedded Switch
Brocade VA-40FC switch	8 Gbps 40-port Switch
Brocade 415 Host Bus Adapter	4 Gbps 1-port HBA
Brocade 425 Host Bus Adapter	4 Gbps 2-port HBA
Brocade 815 Host Bus Adapter	8 Gbps 1-port HBA
Brocade 825 Host Bus Adapter	8 Gbps 2-port HBA
Brocade 48000 director	Director Chassis
Brocade 48000 director with FC4-16, FC4-32, and FC4-48 <sup>2</sup> Blades	Director Chassis with 4 Gbps 16-FC port, 4 Gbps 32-FC port, and 4 Gbps 48-FC port
Brocade 48000 director with FR4-18i <sup>1</sup> Blades	Director Chassis with 4 Gbps router, extension blades
Brocade 48000 director with FC4-16IP <sup>2</sup> Blades	Director Chassis with 4 Gbps 8-FC port and 8 GbE iSCSI blades
Brocade 48000 director with FC10-6 <sup>4</sup> Blades	Director Chassis with 10 Gbps 6-port ISL blades

**TABLE 1** Supported Hardware (Continued)

Device Name	Terminology used in documentation
Brocade DCX <sup>7</sup>	384-port Backbone Chassis
Brocade DCX <sup>7</sup> with FC8-16, FC8-32, and FC8-48 Blades	384-port Backbone Chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port blades
Brocade DCX <sup>7</sup> with FR4-18i Blades	384-port Backbone Chassis with 4 Gbps Router, Extension blade
Brocade DCX <sup>9</sup> with FC10-6 Blades	384-port Backbone Chassis with FC 10 - 6 ISL Blade
Brocade DCX <sup>8</sup> with FS8-18 Blades	384-port Backbone Chassis with Encryption Blade
Brocade DCX <sup>12</sup> with FX8-24 Blades	384-port Backbone Chassis with 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade
Brocade DCX <sup>12</sup> with FCoE10-24 Blades	384-port Backbone Chassis with 10 Gbps 24-port FCoE blade
Brocade DCX-4S <sup>7</sup>	192-port Backbone Chassis
Brocade DCX-4S <sup>9</sup> with FC8-16, FC8-32, and FC8-48 Blades	192-port Backbone Chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port blades
Brocade DCX-4S <sup>9</sup> with FR4-18i Blades	192-port Backbone Chassis with 4 Gbps Router, Extension blade
Brocade DCX-4S <sup>9</sup> with FC10-6 Blades	192-port Backbone Chassis with FC 10 - 6 ISL Blade
Brocade DCX-4S <sup>9</sup> with FS8-18 Blades	192-port Backbone Chassis with Encryption Blade
Brocade DCX-4S <sup>12</sup> with FX8-24 Blades	192-port Backbone Chassis with 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade
Brocade DCX-4S <sup>11</sup> with FCoE10-24 Blades	192-port Backbone Chassis with 10 Gbps 24-port FCoE blade
Brocade Encryption Switch <sup>8</sup>	8 Gbps Encryption Switch
FS8-18 Encryption Blade	Encryption Blade
FA4-18 Application Platform Blade	Application Platform Blade
FC8-16 Blade	FC 8 GB 16-port Blade
FC8-32 Blade	FC 8 GB 32-port Blade
FC8-48 Blade	FC 8 GB 48-port Blade
FC10-6 Blade	FC 10 - 6 ISL Blade
FCoE10-24 Blade	10 Gig FCoE Port Router Blade
FX8-24 Blade	8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension Blade
M4700F Fabric Switch	32-Port, 4 Gbps Switch
M6140 Director	140-Port Director

**TABLE 1** Supported Hardware (Continued)

Device Name	Terminology used in documentation
Mi10K Director	256-Port Director
1 Platform requires Fabric OS v5.1.0 or later	
2 Platform requires Fabric OS v5.2.0 or later	
3 Platform requires Fabric OS v5.2.1 or later	
4 Platform requires Fabric OS v5.3.0 or later	
5 Platform requires Fabric OS v5.3.1 or later	
6 Platform requires Fabric OS v6.1.0 or later	
7 Platform requires Fabric OS v6.0.0 or later	
8 Platform requires Fabric OS v6.1.1_enc or later	
9 Platform requires Fabric OS v6.2.0	
10 Platform requires Fabric OS v6.1.2_CEE	
11 Platform requires Fabric OS v6.3.0 or later	
12 Platform requires Fabric OS v6.3.1_CEE	

## Supported open source software products

[Table 2](#) lists the open source software third-party software products used in DCFM 10.4.0.

**TABLE 2** Supported Open Source Software Third-party Software Products

Open Source Software Product	License Type
ApacheFTPServer n/a	Apache
BouncyCastleCryptoPackage 1.38	Bouncy Castle
Derby 10.3.2.1	Apache
DroolsBusinessRuleManagementSystemBRMS 4.0.4	LGPL
EnterpriseDTFTP 1.5.6	LGPL
GoogleGuice 1	Apache
iBATISDAOFramework 2.2.0	Apache
iBATISforJava 2.3.0	Apache
iText 2.0.7	LGPL
JasperReports 2.0.2	LGPL
JavaTar2.5andTarTool1.4 2.5/1.4	public domain
JbossApplicationServer 4.2.2	LGPL
JbossMessaging 1.4.5.GA	LGPL
JDOM 1.1	Apache (with acknowledgment clause removed)
JFreeChart 1.0.8a	LGPL
Jmesa 2.4.5	Apache
JradiusClient 2	LGPL

**TABLE 2** Supported Open Source Software Third-party Software Products (Continued)

Open Source Software Product	License Type
JRE 1.6	Sun License
Log4j 1.2	Apache
QuartzEnterpriseJobScheduler 1.6.0	Open Source
TheJavaCIFSCClientLibrary 1.2.17	LGPL
TrileadSSHforJava 2.0.2	Trilead AG
VJJava2 2.0	BSD License
XMLRPC 1.2-B1	Open Source
ApachecommonsPool 1.5.4	Open Source
ApachecommonsDBCP 1.2.2	Open Source

## What's new in this document

The following changes have been made since this document was last released:

- Information that was added:
  - Added View All list
  - Added Export to Toolbox
  - Added CNA icons
  - Added procedure - Clearing previous version of the remote client
  - Added procedure - Launching the Configuration Wizard
  - Added procedure - Installing a patch
  - Added procedure - Uninstalling a patch
  - Added topic - VMware vCenter plug in
  - Added topic SMIA Configuration tool
  - Added procedure - Exporting storage port mapping
  - Added procedure - Copying technical support information to an external FTP server
  - Added procedure - Setting up advanced event filtering for the Master Log
  - Added procedure - Removing an advanced event filter
  - Added Managed CNA Ports to Performance chapter
  - Added Firmware download troubleshooting
  - Added Launch Client troubleshooting
  - Added Performance troubleshooting
  - Added Port Fencing troubleshooting
  - Added Server Management Console troubleshooting
  - Added View All list troubleshooting
  - Added privilege - SMIA Operations

- Information that was changed:
  - Changed View tab to SAN tab
  - Moved Menu bar table to Appendix
  - Changed AG icons
  - Moved Management server and client section to Chapter 1 Getting Started
  - Changed procedure - Discovering a fabric
  - Changed topic - Fabric Monitoring
  - Changed topic - seed switch failover
  - Moved Call Home to new chapter
  - Moved View Management and Topology to new chapter
  - Moved Third party tools to new chapter
  - Changed topic - Fabric tracking
  - Changed SAN menu to Server menu
  - Changed procedure - Backing up a switch configuration
  - Changed procedure - Download firmware
  - Changed HBA Sever Mapping to Host Port Mapping
  - Changed procedure - Scheduling technical support information collection
  - Changed procedure - Starting immediate technical support information collection
  - Changed procedure - Launching scripts
  - Changed procedure - Setting up advanced event filtering for a user
  - Changed topic - Syslog forwarding
  - Changed Top Talkers dialog box
  - Changed topic - Thresholds and event notification
  - Moved Reports from Monitor menu to menu bar
  - Made Port Fencing a chapter
  - Changed procedure - Viewing the list of users
  - Changed procedure - Assigning a user to a resource group
  - Changed procedure - Removing a user from a resource group
  - Changed procedure - Activating a PDCM configuration
  - Changed topic - Cascaded FICON fabric
  - Changed procedure - Configuring a cascaded FICON fabric
  - Changed procedure - Cascaded FICON fabric merge
  - Changed topic - Port Groups
  - Changed procedure - Adding a detached device
  - Changed Supportsave troubleshooting
  - Changed topic - Privileges and Application Behavior table
- Information that was deleted:
  - Removed EMC E-mail and HP Modem call home centers.

For further information about new features and documentation updates for this release, refer to the release notes.

## Document conventions

This section describes text formatting conventions and important notice formats used in this document.

### Text formatting

The narrative-text formatting conventions that are used are as follows:

<b>bold text</b>	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
<i>italic text</i>	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
<code>code text</code>	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is all lowercase.

### Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

---

#### NOTE

A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

---

---

#### ATTENTION

An Attention statement indicates potential damage to hardware or data.

---

### Key terms

For definitions specific to Brocade and Fibre Channel, see the *Brocade Glossary*.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

<http://www.snia.org/education/dictionary>

## Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Linus Torvalds	Linux
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Netscape Communications Corporation	Netscape
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover
Sun Microsystems, Inc.	Sun, Solaris, Sun Fire, Sun Ultra, Java Plug-in
The Open Group	UNIX
VMware, Inc.	VMware

## Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

### Brocade resources

To get up-to-the-minute information, go to <http://my.brocade.com> to register at no cost for a user ID and password.

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

<http://www.amazon.com>

White papers, online demonstrations, and data sheets are available through the Brocade website at:

<http://www.brocade.com/products-solutions/products/index.page>

For additional Brocade documentation, visit the Brocade website:

<http://www.brocade.com>

Release notes are available on the MyBrocade website and are also bundled with the Fabric OS firmware.

## Other industry resources

For additional resource information, visit the Technical Committee T11 website. This website provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

<http://www.t11.org>

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association website:

<http://www.fibrechannel.org>

## Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. DCFM Serial Number

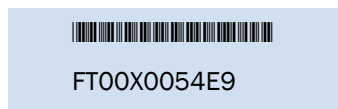
To obtain the DCFM serial number, select **Help > License**. The **DCFm License** dialog box displays.

2. General Information

- Switch model
- Switch operating system version
- Error numbers and messages received
- **supportSave** command output
- Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
- Description of any troubleshooting steps already performed and the results
- Serial console and Telnet session logs
- syslog message logs

3. Switch Serial Number

The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below:



The serial number label is located as follows:

- *Brocade 200E*—On the nonport side of the chassis
- *Brocade 300, 4100, 4900, 5100, 5300, 7500, 7800, 8000, VA-40FC, and Brocade Encryption Switch*—On the switch ID pull-out tab located inside the chassis on the port side on the left
- *Brocade 5000*—On the switch ID pull-out tab located on the bottom of the port side of the switch

- *Brocade 7600*—On the bottom of the chassis
- *Brocade 48000*—Inside the chassis next to the power supply bays
- *Brocade DCX and DCX-4S*—On the bottom right on the port side of the chassis

4. World Wide Name (WWN)

Use the **wwn** command to display the switch WWN.

If you cannot use the **wwn** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

## Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

[documentation@brocade.com](mailto:documentation@brocade.com)

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

## About This Document

# Getting Started

---

## In this chapter

- User interface components ..... 1
- Icon legend..... 11
- Management server and client..... 14
- License..... 25
- Feature-to-firmware requirements ..... 29
- Accessibility features for the Management application ..... 31

## User interface components

The Management application provides easy, centralized management of the SAN, as well as quick access to all product configuration applications. Using this application, you can configure, manage, and monitor your networks with ease.

The Management application's main window contains a number of areas. The following graphic illustrates the various areas, and descriptions of them are listed below.

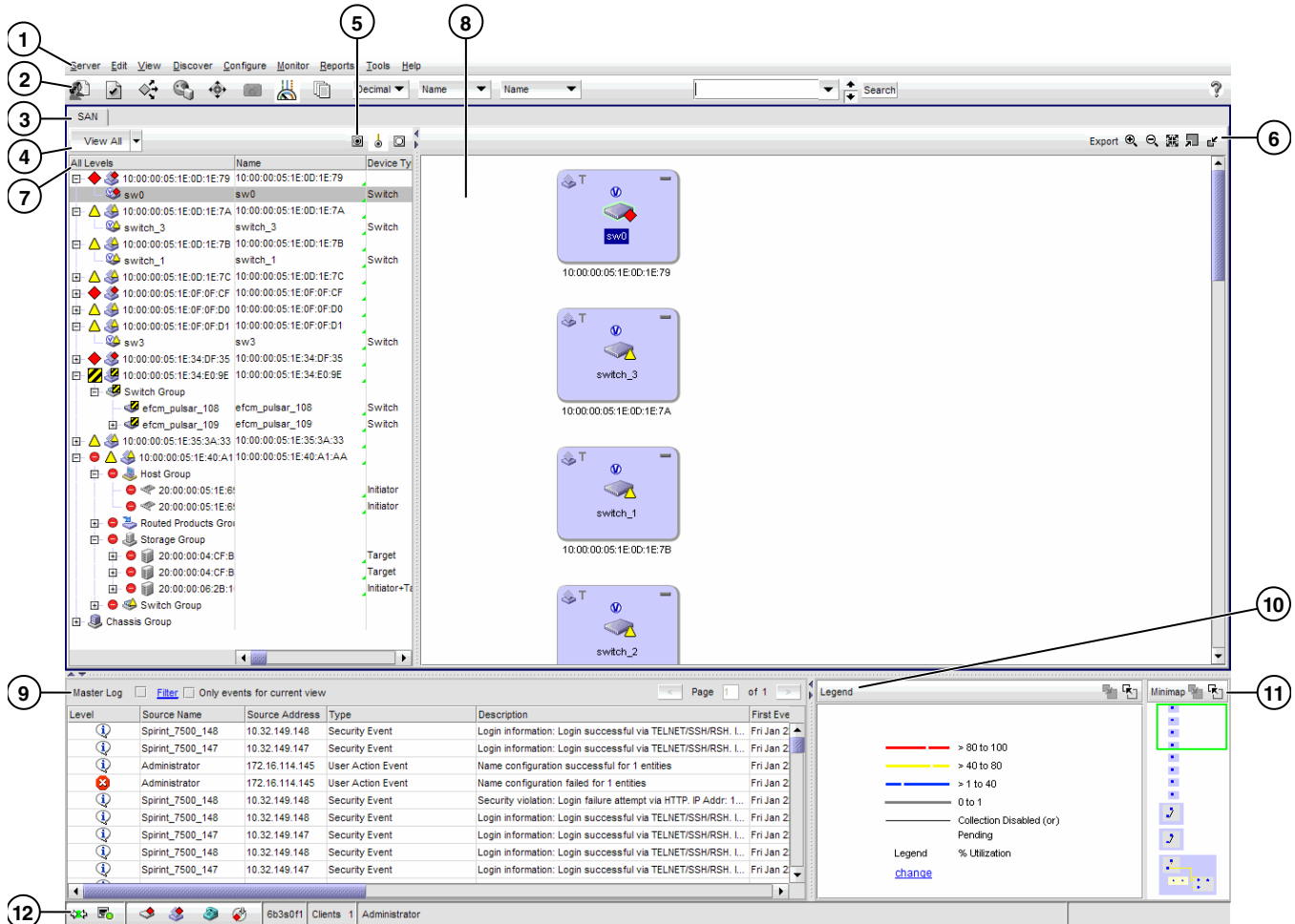
---

### NOTE

Some panels may be hidden by default. To view all panels, select **View > Show Panels > All Panels**, or press **F12**.

---

# 1 User interface components



**FIGURE 1 Main Window**

- Menu Bar.** Lists commands you can perform on the SAN.
- Toolbar.** Provides buttons that enable quick access to dialog boxes and functions.
- SAN tab.** Displays the Master Log, Minimap, Connectivity Map (topology), and Product List. For more information, refer to the “SAN tab”.
- View All list.** Enables you to create, copy, or edit a view, select to how to view the Product list (All Levels, Products and Ports, Products Only, or Ports Only) and to select which view you want to display in the main window. Does not display until you discover a fabric.
- Port Display buttons.** Provides buttons that enable quick access to configuring how ports display. Does not display until you discover a fabric. For more information, refer to “Port Display buttons” on page 5.
- Product List.** Lists the devices discovered in the SAN.
- Connectivity Map.** Displays the SAN topology, including discovered and monitored devices and connections.

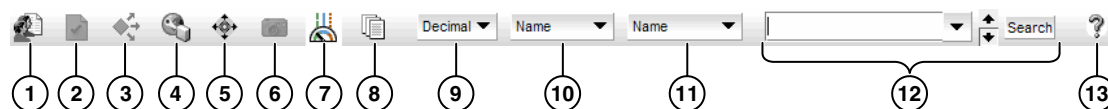
8. **Toolbox.** Provides tools for viewing the Connectivity Map as well as exporting the Connectivity Map as an image. Does not display until you discover a fabric.
9. **Master Log.** Displays all events that have occurred on the SAN.
10. **Utilization Legend.** (Enterprise edition only) Indicates the percentage ranges represented by the colored, dashed lines on the Connectivity Map. Only displays when you select **Monitor > Performance > View Utilization** or click the **Utilization** icon on the toolbar.
11. **Minimap.** Displays a “bird’s-eye” view of the entire SAN. Does not display until you discover a fabric.
12. **Status Bar.** Displays data regarding the Server, connection, device, and fabric.

## Menu bar

The menu bar is located at the top of the main window. For a list of the many functions available on each menu, refer to “[Main menus](#)” on page 675.

## Toolbar

The toolbar is located at the top of the main window and provides icons to perform various functions ([Figure 2](#)).



**FIGURE 2** The Toolbar

The icons on your toolbar will vary based on the licensed features on your system.

1. **Users.** Displays the **Server Users** dialog box. Use to configure users, user groups, and permissions.
2. **Properties.** Displays the **Properties** dialog box of the selected device or fabric. Use to view or edit device or fabric properties.
3. **Launch Element Manager.** Launches the Element Manager of the selected device. Use to configure a device through its Element Manager.
4. **Discover Setup.** Displays the **Discover Setup** dialog box. Use to configure discovery.
5. **Zoning.** Displays the **Zoning** dialog box. Use to configure zoning.
6. **Track Fabric Changes.** Select to turn track fabric changes off for the selected device or group.
7. **View Utilization.** Displays or hides the utilization legend.
8. **View Report.** Displays the **View Reports** dialog box. Use to view available reports.
9. **Domain ID/Port #.** Use to set the domain ID or port number to display as decimal or hex in the Connectivity Map.
10. **Product Label.** Use to set the product label for the devices in the Connectivity Map.

11. **Port Label.** Use to set the port label for the devices in the Connectivity Map.
12. **Product List Search.** Use to search for a device in the product list.
13. **Help.** Displays the Online Help.

## SAN tab

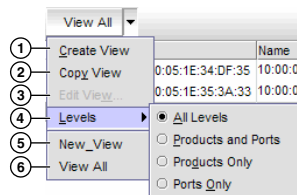
The **SAN** tab displays the Master Log, Utilization Legend, Minimap, Connectivity Map (topology), and Product List.

To open all areas of the **View** window, select **View > Show Panels > All Panels** or press **F12**.

You can change the default size of the display by placing the cursor on the divider until a double arrow displays. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.

## View All list

The **View All** list is located at the top left side of the window and enables you to create, copy, or edit a view, select to how to view the Product list (All Levels, Products and Ports, Products Only, or Ports Only) and to select which view you want to display in the main window. Does not display until you discover a fabric. To discover a fabric, refer to [“Discovering fabrics”](#) on page 36.



**FIGURE 3** View All list

1. **Create View.** Select to create a new view.
2. **Copy View.** Select to copy an existing view.
3. **Edit View.** Select to edit an existing view.
4. **Levels.** Select the level at which you want to view the Product list, Options include: All Levels, Products and Ports, Products Only, or Ports Only.
5. **View\_Name.** Any additional views that you create. Select which view you want to display in the main window.
6. **View All.** Select to display the default view of the main window.

## Port Display buttons

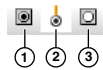
The **Port Display** buttons (Figure 4) are located at the top right of the Product List and enable you to configure how ports display. You have the option of viewing connected (or occupied) product ports, unoccupied product ports, or attached ports. Does not display until you discover a fabric.

---

### NOTE

Occupied/connected ports are those that originate from a device, such as a switch. Attached ports are ports of the target devices that are connected to the originating device.

---



**FIGURE 4** Port Display buttons

1. **Occupied Product Ports.** Displays the ports of the devices in the fabrics (present in the connectivity map) that are connected to other devices.
2. **Unoccupied Product Ports.** Displays the ports of the devices (shown in the connectivity map) that are not connected to any other device.
3. **Attached Ports.** Displays the attached ports of the target devices.

## Product List

The Product List, located on the **SAN** tab, displays an inventory of all discovered devices and ports. The Product List is a quick way to look up product and port information, including serial numbers and IP addresses.

To display the Product List, select **View > Show Panels > Product List** or press **F9**.

You can edit information in the Product List by double-clicking in a field marked with a green triangle. You can sort the Product List by clicking a column heading.

The following columns (presented here in alphabetical order) are included in the Product List.

- **Additional Port Info.** Displays additional port information.
- **All Levels.** Displays all discovered fabrics, groups, devices, and ports as both text and icons. Also, displays the status of the fabrics, groups, devices, and ports. For a list of icons that display in the **All Levels** column, refer to the following tables:
  - “[Product icons](#)” on page 11
  - “[Group icons](#)” on page 12
  - “[Port icons](#)” on page 12
  - “[Product status icons](#)” on page 13
- **Attached Port #.** Displays the number of the attached port.
- **BB Credit.** Displays the BB Credit of the port.
- **Class.** Displays the class value of the FICON device port.
- **Contact.** Displays the name of the person or group you should contact about the product. This field is editable at the fabric level.
- **Description.** Displays the description of the product. This field is editable at the fabric level.
- **Device Type.** Displays the type of device.

- **Domain ID.** Displays the Domain ID for the product in the format xx(yy), where xx is the normalized value and yy is the actual value on the wire.
- **FC Address.** Displays the Fibre Channel address of the port.
- **Firmware.** Displays the firmware version of the product.
- **IP Address.** Displays the IP address (IPv4 or IPv6 format) of the product.
- **Location.** Displays the physical location of the product. This field is editable at the fabric level.
- **Model.** Displays the model number of the product.
- **Name.** Displays the name of the product. This field is editable at the fabric, device, and port level.
- **Port #.** Displays the number of the port.
- **Port Count.** Displays the number of ports on the product.
- **Port Type.** Displays the type of port (for example, expansion port, node port, or NL\_port).
- **Protocol.** Displays the protocol for the port.
- **Serial #.** Displays the serial number of the product.
- **Speed Configured (Gbps).** Displays the actual speed of the port in Gigabits per second.
- **State.** Displays the state for the product and the port.
- **Status.** Displays the status for the product and the port.
- **Symbolic Name.** Displays the symbolic name for the port.
- **TAG.** Displays the tag number of the product.
- **Vendor.** Displays the name of the product's vendor.
- **WWN.** Displays the world wide name of the product or port.

## Connectivity Map

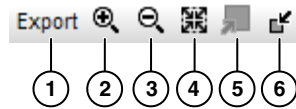
The Connectivity Map, which displays in the upper right area of the main window, is a grouped map that shows physical and logical connectivity of SAN components, including discovered and monitored devices and connections. These components display as icons in the Connectivity Map. For a list of icons that display in the Connectivity Map, refer to the following tables:

- [“Product icons”](#) on page 11
- [“Group icons”](#) on page 12
- [“Product status icons”](#) on page 13

The Management application displays all discovered fabrics in the Connectivity Map by default. To display a discovered Host in the Connectivity Map, you must select the Host in the Product List. You can only view one Host and physical and logical connections at a time.

## Toolbox

The toolbox ([Figure 5](#)) is located at the top right side of the **View** window and provides tools to export the topology, to zoom in and out of the Connectivity Map, collapse and expand groups, and fit the topology to the window. Does not display until you discover a fabric.



**FIGURE 5** The Toolbox

1. **Export.** Use to export the topology to a PNG file.
2. **Zoom In.** Use to zoom in on the Connectivity Map
3. **Zoom Out.** Use to zoom out on the Connectivity Map.
4. **Fit in View.** Use to scale the map to fit within the Connectivity Map area.
5. **Expand.** Use to expand the map to show all ports in use on a device.
6. **Collapse.** Use to collapse the map to show only devices (hides ports).

## Master Log

The Master Log, which displays in the lower left area of the main window, lists the events and alerts that have occurred on the SAN. If you do not see the Master Log, select **View > Show Panels > All Panels** or press **F5**.

You can sort the Master Log by clicking a column heading. By default, the Master Log is sorted by the **Last Event Server Time** column. To filter information in the Master Log, refer to [“Filtering events in the Master Log”](#) on page 253.

The following fields and columns are included in the Master Log:

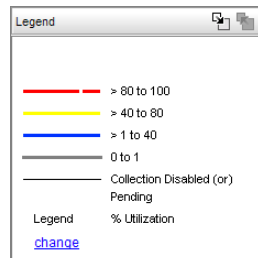
- **Level.** The severity of the event. When the same event (Warning or Error) occurs repeatedly, the Management application automatically eliminates the additional occurrences. For more information about events, refer to [“Fault Management”](#) on page 247. For a list of the event icons, refer to [“Event icons”](#) on page 13.
- **Source Name.** The product on which the event occurred.
- **Source Address.** The IP address (IPv4 or IPv6 format) of the product on which the event occurred.
- **Type.** The type of event that occurred (for example, client/server communication events).
- **Description.** A description of the event.
- **First Event Server Time.** The time and date the event first occurred on the server.
- **Last Event Server Time.** The time and date the event last occurred on the server.
- **First Event Product Time.** The time and date the event first occurred on the product.
- **Last Event Product Time.** The time and date the event last occurred on the product.
- **Operational Status.** The operational status (such as, unknown, healthy, marginal, or down) of the product on which the event occurred.

# 1 Utilization Legend

- **Count.** The number of times the event occurred.
- **Module Name.** The name of the module on which the event occurred.
- **Message ID.** The message ID of the event.
- **Contributor.** The name of the contributor on which the event occurred.
- **Node WWN.** The world wide name of the node on which the event occurred.
- **Fabric Name.** The name of the fabric on which the event occurred.

## Utilization Legend

The Utilization Legend, which displays in the lower right corner of the main window, indicates the percentage ranges represented by the colored, dashed lines on the Connectivity Map. It only displays when you select **Monitor > Performance > View Utilization** or click the **Utilization** icon on the toolbar.



**FIGURE 6** Utilization Legend

The colors and their meanings are outlined in the following table.

Line Color	Utilization Defaults
Red line	80% to 100% utilization
Yellow line	40% to 80% utilization
Blue line	1% to 40% utilization
Gray line	0% to 1% utilization
Black line	Utilization disabled

For more information about the utilization legend, refer to [“Connection utilization”](#) on page 315.

## Minimap

The **Minimap**, which displays in the lower right corner of the main window, is useful for getting a bird's-eye view of the SAN, or to quickly jump to a specific place on the Connectivity Map. To jump to a specific location on the Connectivity Map, click that area on the Minimap. A close-up view of the selected location displays on the Connectivity Map.

Use the Minimap to view the entire SAN and to navigate more detailed map views. This feature is especially useful if you have a large SAN. Does not display until you discover a fabric.

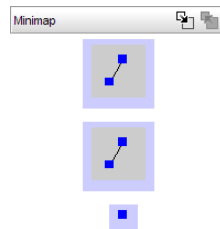


FIGURE 7 Minimap

### *Anchoring or floating the Minimap*

You can anchor or float the Minimap to customize your main window.

- To float the Minimap and view it in a separate window, click the **Detach** icon (📄) in the upper right corner of the Minimap.
- To anchor the Minimap and return the Minimap to its original location on the main window, do one of the following steps:
  - Click the **Attach** icon (📄) in the upper right corner of the Minimap.
  - Click the **Close** icon (✕) in the upper right corner of the Minimap.
  - Double-click the logo in the upper left corner of the Minimap.
  - Click the logo in the upper left corner of the Minimap and select **Close** (ALT + F4).

### *Resizing the Minimap*

On an anchored Minimap, place the cursor on the left border of the Minimap until a double-pointed arrow displays. Click and drag the adjoining divider.

On a floating Minimap, place the cursor on a border of the Minimap until a double-pointed arrow displays. Click and drag to change the window size.

## Status bar

The status bar (Figure 8) displays at the bottom of the main window. The status bar provides a variety of information about the SAN and the application. The icons on the status bar change to reflect different information, such as the current status of products, fabrics, and backup.

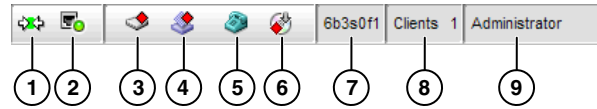


FIGURE 8 Status Bar

The icons on your status bar will vary based on the licensed features on your system.
























1. **Connection Status.** Displays the Server-Client connection status.
2. **Port Status.** Displays port status for the following ports: SNMP, Syslog, FTP, and Web Server.
3. **Product Status.** Displays the status of the most degraded device in the SAN. For example, if all devices are operational except one (which is degraded), the Product Status displays as degraded. Click this icon to open the **Product Status Log**.
4. **Fabric Status.** Displays the state of the fabric that is least operational, based on ISL status. The possible states are: operational, unknown, degraded or failed. Select a product or fabric from the Connectivity Map or Product List and click this icon to open the related **Fabric Log** (only available for persisted fabrics).
5. **Call-Home Status.** (Enterprise edition only) Displays a call home status icon when one or more fabrics are discovered, which allows you to determine the current call home status. For more information about Advanced Call Home status and icons, refer to [“Viewing Call Home status”](#) on page 117.
6. **Backup Status.** Displays a backup status icon, which allows you to determine the current backup status. Let the pointer pause on the backup status icon to display the following information in a tooltip.
  - **Backup in Progress icon.** Backup started at hh:mm:ss, in progress... XX files in *Directory\_Name* are backed up.
  - **Countdown to Next Scheduled Backup icon.** Waiting for next backup to start.
  - **Backup Disabled icon.** Backup is disabled.
  - **Backup Failed icon.** Backup failed at hh:mm:ss mm/dd/yyyy.
7. **Server Name.** Displays the name of the Server to which you are connected.
8. **Total Users.** Displays the number of clients logged into the server.
9. **User’s ID.** Displays the user ID of the logged in user.

## Icon legend

Various icons are used to illustrate devices and connections in a SAN. The following tables list icons that display on the Connectivity Map and Product List.







### Product icons

The following table lists the manageable SAN product icons that display on the topology. Fabric OS manageable devices display with blue icons and M-EOS manageable devices display with green icons. If a device is unmanageable it displays with gray icons. Some of the icons shown display when certain features are licensed.

Icon	Description	Icon	Description
	Fabric		Fabric OS Switch and Blade Switch
	Fabric OS Director		Fabric OS CEE Switch
	Fabric OS Router		Storage
	Fabric OS FC Switch in Access Gateway mode (single-fabric connected)		Fabric OS FC Switch in Access Gateway mode (multiple-fabric connected)
	Fabric OS CEE Switch in Access Gateway mode (single-fabric connected)		Fabric OS CEE Switch in Access Gateway mode (multiple-fabric connected)
	M-EOS Switch		M-EOS Director
	iSCSI Target		iSCSI Initiator
	HBA		HBA Mezzanine Card
	CNA HBA		CNA Mezzanine Card
	Unmanaged HBA		Host
	VM Host		Unmanaged Host
	Ethernet Cloud		












## Group icons

The following table lists the manageable SAN product group icons that display on the topology.

Icon	Description	Icon	Description
	Switch Group		Host Group
	Storage Group		Unknown Fabric Group
	Unmanaged Fabric Group		Chassis Group









## Port icons

The following table lists the port status icons that display in the Product List.

Icon	Description
	Occupied FC Port
	Unoccupied FC Port
	Attached FC Port
	Trunk (port group)
	IP and 10 GE Port
	Attached IP and 10 GE Port
	Attached-to-Cloud 10 GE Port
	Virtual Port
	Virtual FCoE Port
	Attached FCoE Port
	Pre-boot Virtual Port




## Product status icons

The following table lists the product status icons that display on the topology.

Icon	Status
No icon	Healthy/Operational
	Attention
	Degraded/Marginal
	Device Added
	Device Removed/Missing
	Down/Failed
	Routed In
	Routed Out
	Unknown/Link Down

## Event icons

The following table lists the event icons that display on the topology and Master Log. For more information about events, refer to [“Fault Management”](#) on page 247.

Event Icon	Description
	Informational
	Warning
	Error

## Management server and client

The Management application has two parts: the Server and the Client. The Server is installed on one machine and stores SAN-related information; it does not have a user interface. To view SAN information through a user interface, you must log in to the Server through a Client. The Server and Clients may reside on the same machine, or on separate machines.

In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between Servers and Clients. In other words, a Client can find a Server, appear to log in, but is immediately logged out because the Server cannot reach the Client. To resolve this issue, check to determine if the ports in the table below need to be opened up in the firewall.

**TABLE 3** Ports

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
20 <sup>1</sup>	FTP Port (Control)	TCP	FTP Control port for internal FTP server	Client-Server Switch-Server	Yes Yes
21 <sup>1, 2</sup>	FTP Port (Data)	TCP	FTP Data port for internal FTP server	Client-Server Switch-Server	Yes Yes
22 <sup>1</sup>	SSH or Secure Telnet	TCP	Sectelnet port from server to switch/client to switch	Server-Switch Client-Switch	Yes
23 <sup>1</sup>	Telnet	TCP	Telnet port from server/client to switch	Server-Switch Client-Switch	Yes
25	SMTP Server port	TCP	SMTP Server port for E-mail communication	Server-SMTP Server	Yes
80	jboss.web.http.port	TCP	Non-SSL HTTP/1.1 connector port	Client-Server	Yes
80 <sup>3, 4</sup>	Switch http	TCP	Switch non-SSL http port for http and CAL communication	Server-Switch Client-Switch	Yes
161 <sup>1</sup>	SNMP Port	UDP	Default SNMP port	Server-Switch	Yes
162 <sup>3</sup>	snmp.trap.port	UDP	Default SNMP trap port	Switch-Server	Yes
389	LDAP Server Port	TCP	LDAP server port for authentication if LDAP is chosen as an external authentication	Server-LDAP Server	Yes
443 <sup>3, 4, 5</sup>	Switch https	TCP	Switch SSL http port for https and CAL communication	Server-Switch Client-Switch	Yes
514 <sup>6</sup>	Syslog Port	UDP	Default Syslog Port	Switch-Server	Yes
1024 <sup>1, 7</sup>	MPI	TCP	MPI trap recipient port	Switch-Server	Yes
1812	RADIUS Server Port	UDP	RADIUS server port for authentication if RADIUS is chosen as an external authentication	Server-RADIUS Server	Yes
2048 <sup>1, 9</sup>	MPI	TCP	MPI discovery NMRU port	Server-Switch	Yes
2049 <sup>1, 5, 7, 9</sup>	MPI	TCP	MPI discovery NMRU port for SSL	Server-Switch	Yes

**TABLE 3** Ports (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
2638 <sup>8</sup>	Database port (Enforced during install)	TCP	Port used by database	Server–Database Remote ODBC– Database	Yes
4430 <sup>1, 5, 7</sup>	MPI	TCP	XML-RCP port for SSL	Server–Switch	Yes
8080 <sup>1, 7</sup>	MPI	TCP	XML-RCP port/HTTP port	Server–Switch	Yes
24600 <sup>10</sup>	jboss.naming.jnp.port - port 0	TCP	Bootstrap JNP service port	Client–Server	Yes
24601	jboss.connector.ejb3.port - port 1	TCP	EJB3 connector port	Client–Server	Yes
24602	jboss.connector.bisocket.port - port 2	TCP	Bisocket connector port	Client–Server	Yes
24603	jboss.connector.bisocket.secondary.port - port 3	TCP	Bisocket connector secondary port	Client–Server	Yes
24604 <sup>5</sup>	jboss.connector.sslbisocket.port - port 4	TCP	SSL Bisocket connector port	Client–Server	Yes
24605 <sup>5</sup>	jboss.connector.sslbisocket.secondary.port - port 5	TCP	SSL Bisocket connector secondary port	Client–Server	Yes
24606	smp.registry.port - port 6	TCP	RMI registry port	Client–Server	Yes
24607	smp.server.export.port - port 7	TCP	RMI export port	Client–Server	Yes
24608	smp.server.cliProxyListening port - port 8	TCP	CLI proxy telnet port	Client–Server	Yes
24609	jboss.naming.rmi.port - port 9	TCP	RMI naming service port	Client–Server	Yes
24610	jboss.jrmp.invoker.port - port 10	TCP	RMI/JRMP invoker port	Client–Server	Yes
24611	jboss.pooled.invoker.port - port 11	TCP	Pooled invoker port	Client–Server	Yes
24612	jboss.connector.socket.port - port 12	TCP	Socket invoker port	Server	No
24613	jboss.web.ajp.port - port 13	TCP	AJP 1.3 connector port	Server	No
24614	jboss.web.service.port - port 14	TCP	Web service port	Server	No
24615	connector.bind.port - port 15	TCP	Port to listen for requests on	Server	No
55555 <sup>10</sup>	Client Export Port	TCP	Client port to which server pushes the M-EOS device Element Manager updates	Server–Client	Yes

# 1 Management server and client

**TABLE 3** Ports (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
55556	Launch in Context (LIC) client hand shaking port	TCP	Client port used to check if a Management application client opened using LIC is running on the same host  <b>NOTE:</b> If this port is in use, the application uses the next available port.	Client	No
1	Port is not configurable (either in the switch or the Management server).				
2	Every FTP session requires an additional port which is randomly picked. If the firewall is enabled then FTP operation (used for firmware download, technical support, firmware import (from client-server) and so on.) will fail.				
3	Ports configurable in the switch and the Management server. Port must be the same for all switches managed by the Management server.				
4	Ports used to launch the Web Tools application for Fabric OS switches from the Management client. This is applicable only when the Fabric OS version is earlier than 6.1.1.				
5	Port used for SSL communication. If SSL is enabled, you must open 443*, 24604, and 24605 in the firewall. If SSL is not enabled, port 80* must be open in the firewall and 443*, 24604, and 24605 can be closed. An asterisk (*) denotes the default web server port number. If you set the web server port number to a port other than the default, you must open that port in the firewall.				
6	The Syslog listening port is configurable in the Management server. The switch always sends syslog messages to port 514. If you have any other syslog daemon on the Management server machine already listening to 514, then the Management Server can be configured to listen to a different port. You must manually configure relay in existing syslogd to forward the syslog messages to the Management Server listening on the configured port.				
7	Ports used for communicating with M-EOSn (M-i10K) directors. M-i10K always uses NMRU over SSL (2049). M-i10K always uses 8080 for http requests (firmware download, configuration backup/ restore, data collection). If M-EOSn firmware version is less than 9.1 the Management application uses 8080 for XML-RPC requests (discovery and asset collection). If the M-EOSn firmware version is more than 9.1 then it always uses SSL port (4430) for XML-RPC.				
8	Port must be opened in firewall for the server when the remote ODBC client needs to talk to the Management database server (Only for EE). The same port is used by the Management server to database server (local). This is not used by the Management client.				
9	Ports used for communicating with M-EOS (excluding M-i10K) switches (only required when the Management server manages M-EOS switches).				
10	Port should be opened in firewall in the Management client to allow communication between server and client (only applicable for M-EOS switches). If this port is not opened in the firewall, then the M-EOS element manager does not receive updates. Also if multiple clients are opened, it will try to use the next available port (55556). So if there are n clients opened in the same machine then you must open 55555 (configurable) to 55555 + n ports in the firewall.				
11	The Management server tries to find a contiguous block of 16 ports from the starting port configured (for example, 24600); if any port in this range is not available for the Management application, then you must provide a new starting port. Note that Port 1 to Port 15 in "Ports" column of the table above are not separately configurable and those ports vary based on the starting port number configuration (specified as Port 0 in the above table). The port numbers mentioned in the table above are the default ports (for example, when 24600 is selected as the starting port number).				

## Logging into a server

You must log into a Server to monitor a SAN.

### NOTE

You must have an established user account on the Server to log in.

To log into a server, complete the following steps.

1. Double-click the desktop icon or open the application from the **Start** menu.

The **Log In** dialog box displays (Figure 9).

**FIGURE 9** Log In dialog box

2. Enter your user name and password.

The defaults are **Administrator** and **password**, respectively. If you migrated from a previous release, your username and password do not change.

3. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
4. Click **Login**.
5. Click **OK** on the **Login Banner** dialog box.

The Management application displays.

## Launching a remote client

To launch a remote client, complete the following steps.

1. Open a web browser and enter the IP address of the Management application server in the **Address** bar.

If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP\_Address:Port\_Number*.

The Management application web start screen displays.

2. Click the Management application web start link.

The **Log In** dialog box displays.

3. Enter your user name and password.

The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

## 1 Clearing previous versions of the remote client

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
5. Click **Login**.
6. Click **OK** on the **Login Banner** dialog box.

The Management application displays.

## Clearing previous versions of the remote client

The remote client link in the **Start** menu does not automatically upgrade when you upgrade the Management application. You must clear the previous version from the Java cache.

To clear the Java cache, complete the following steps.

1. Select **Start > Settings > Control Panel > Java**.

The **Java Control Panel** dialog box displays.

2. Click **View** on the **General** tab.

The **Java Cache Viewer** dialog box displays.

3. Right-click the application and select **Delete**.
4. Click **Close** on the **Java Cache Viewer** dialog box.
5. Click **OK** on the **Java Control Panel** dialog box.

To create a remote client link in the **Start** menu, refer to [“Launching a remote client”](#) on page 17.

## Launching the Configuration Wizard

You can re-launch the Configuration wizard to change the following configurations:

- FTP server
- Server IP
- Server Ports
- SMI Agent

---

### NOTE

Changes to these configuration require a server restart.

---

1. Choose one of the following options:
  - On Windows systems, select **Start > Programs > Management\_Application\_Name 10.X.X > Management\_Application\_Name Configuration**.
  - On UNIX systems, execute `sh Install_Home/bin/configwizard` on the terminal.
2. Click **Next** on the **Welcome** screen.
3. Click **Yes** on the confirmation message.

4. Select **Internal FTP Server** or **External FTP Server** on the **FTP Server** screen and click **Next**.

If port 21 is busy, a message displays. Click **OK** to close the message and continue. Once the Management application is configured make sure port 21 is free and restart the Server to start the FTP service.

#### NOTE

If you use an FTP Server which is not configured on the same machine as the Management application, the Firmware Repository feature will not be available.

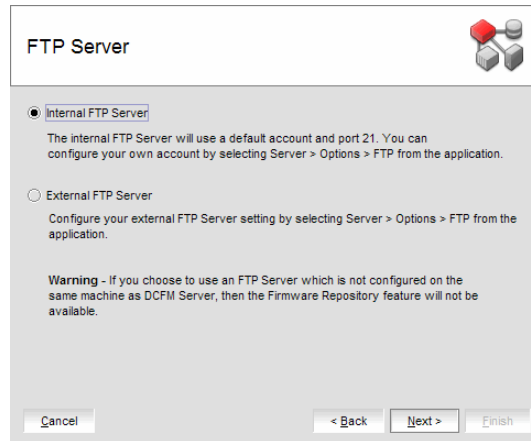


FIGURE 10 FTP Server screen

5. Complete the following steps on the **Server IP Configuration** screen.

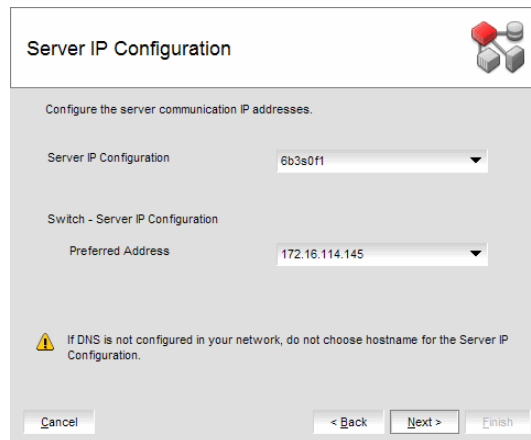


FIGURE 11 Server IP Configuration screen

- a. Select an address from the **Server IP Configuration** list.

# 1 Launching the Configuration Wizard

- b. Select an address from the **Switch - Server IP Configuration Preferred Address** list.

If DNS is not configured for your network, do not select the 'hostname' option from either the **Server IP Configuration** or **Switch - Server IP Configuration Preferred Address** list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.

If you select a specific IP address from the **Server IP Configuration** screen and the selected IP address changes, you will not be able to connect to the server. To change the IP address, refer to [“Configuring an explicit server IP address”](#) on page 94.

- c. Click **Next**.

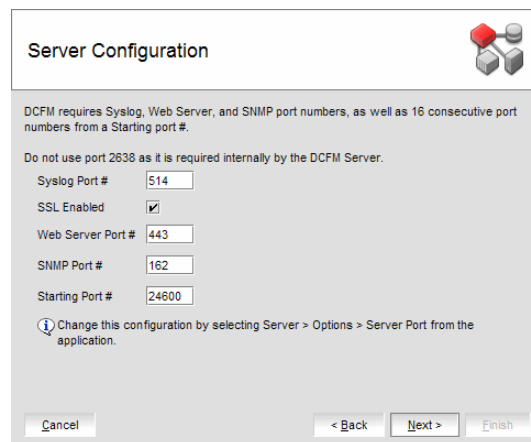
6. Complete the following steps on the **Server Configuration** screen.

---

## NOTE

Do not use port 2638 for any of these port numbers. Port 2638 is used internally by the server.

---



**FIGURE 12** Server Configuration screen

- a. Enter a port number in the **Syslog Port Number** field (default is 514).

---

## NOTE

If the default syslog port number is already in use, you will not receive any syslog messages from the device.

---

- b. Enable SSL by selecting the **SSL Enabled** check box.
- c. Enter a port number in the **Web Server Port Number** field (default is 443 if **SSL Enabled** is selected; otherwise, the default is 80).
- d. Enter a port number in the **SNMP Port Number** field (default is 162).
- e. Enter a port number in the **Starting Port Number** field (default is 24600).

---

## NOTE

The server requires 16 consecutive free ports beginning with the starting port number.

---

- f. Click **Next**.

If you enter a syslog port number already in use, a message displays. Click **No** on the message to remain on the **Server Configuration** screen and edit the syslog port number (return to step 6a). Click **Yes** to close the message and continue with step 7.

If you enter a port number already in use, a Warning displays next to the associated port number field. Edit that port number and click **Next**.

7. Complete the following steps on the **SMI Agent Configuration** screen.

**FIGURE 13 SMI Agent Configuration screen**

- a. Enable the SMI Agent by selecting the **Enable SMI Agent** check box.
- b. Enable the SLP by selecting the **Enable SLP** check box.
- c. Enable the SSL by selecting the **Enable SSL** check box.
- d. Enter the SMI Agent port number in the **SMI Agent Port #** field (default is 5989).
- e. Click **Next**.
8. Verify your configuration information on the **Server Configuration Summary** screen and click **Next**.
9. Complete the following steps on the **Start Server** screen:
  - a. Select the **Start SMI Agent** check box, if necessary.
  - b. Select the **Start SLP** check box, if necessary.
  - c. Select the **Start Client** check box, if necessary.
  - d. Click **Finish**.

After all of the services (Server, SLP, SMI Agent and Client) are started, the **Log In** dialog box displays.

10. Click **Yes** on the restart server confirmation message.
11. Enter your user name and password.

The defaults are **Administrator** and **password**, respectively. If you migrated from a previous release, your user name and password do not change.

# 1 Changing your password

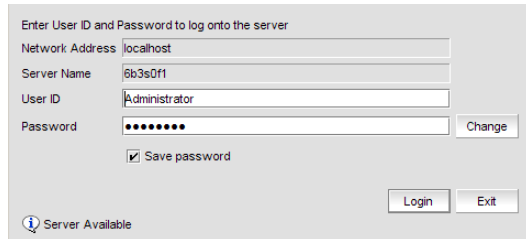
12. Click **Login**.
13. Click **OK** on the Login Banner.

## Changing your password

To change your password, complete the following steps.

1. Double-click the desktop icon or open from the **Start** menu.

The **Log In** dialog box displays.



**FIGURE 14** Log In dialog box

2. Enter your user name and password.

The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

3. Click **Change**.

The **Change Password** dialog box displays.

4. Enter your new password in the **Secure Password** and **Retype Password** fields and click **OK**.
5. Click **Login**.
6. Click **OK** on the **Login Banner** dialog box.

The Management application displays.

## Changing the database user password

To change the database password, complete the following steps in the Install\_Home/bin directory.

1. Open a command window.
2. Type **dbpassword User\_Name Password New\_Password Confirm\_Password** and press **Enter**.

Where *User\_Name* is your user name, *Password* is your current password, and *New\_Password* and *Confirm\_Password* are your new password. The user name and password defaults are dcfm and passwOrd (zero), respectively.

If the password changed successfully, the following message displays:  
Password changed successfully.

If an error occurs and the password did not change, the following message displays:  
Error while updating password. Please try again.  
Press any key to continue.

If the current password and new password are the same, the following message displays:  
Old and New passwords cannot be same. Use different password and try again.  
Press any key to continue.

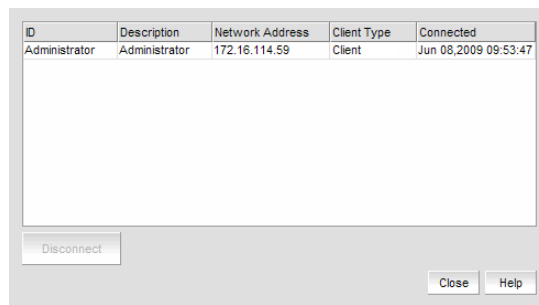
If the new password and confirm password do not match, the following message displays:  
New password and confirm password do not match. Please try again.  
Press any key to continue.

## Viewing active sessions

To view the Management application active sessions, complete the following steps.

1. Select **Server > Active Sessions**.

The **Active Sessions** dialog box displays (Figure 16).



**FIGURE 15** Active Sessions dialog box

2. Review the active session information.

The following information displays:

- **ID**—Displays the name of the user (for example, Administrator).
- **Description**—Displays the description of the user (for example, Operator).
- **Network Address**—Displays the network address of the user.
- **Client Type**—Displays the type of Management application client.
- **Connected**—Displays the date and time the user connected to the server.

3. Click **Close**.

## Disconnecting users

To disconnect a user, complete the following steps.

1. Select **Server > Active Sessions**.

The **Active Sessions** dialog box displays.

2. Select the user you want to disconnect and click **Disconnect**.
3. Click **Yes** on the confirmation message.
4. The user you disconnected receives a 'you have been disconnected' message.
5. Click **Close**.

# 1 Viewing server properties

## Viewing server properties

To view the Management application server properties, complete the following steps.

1. Select **Server > Server Properties**.

The **Server Properties** dialog box displays (Figure 16).

Server Name	6B3S0F1
IP Address	172.16.7.88
Win32 Service	Yes
Started At	05/06/08 9:06:59 AM MDT
Trap Listening Port	162
Java VM Version	1.6.0_03-b05
Java VM Vendor	Sun Microsystems Inc.
Java VM Name	Java HotSpot(TM) Server VM
OS Architecture	x86
OS Name	Windows XP
OS Version	5.1
Region	US
Time Zone	MST
Free Memory	624 MB
Total Memory	757 MB

Close

FIGURE 16 Server Properties dialog box

2. Click **Close**.

## Viewing port status

You can view the port status for the following ports: SNMP, Syslog, FTP, and Web Server.

To view the port status, complete the following steps.

1. Click the port status icon ().

The **Port Status** dialog box displays (Figure 16).

Status field shows whether the port is listening or bound to the server

Name	Port #	Status
SNMP	162	Success
Syslog	514	Success
FTP	21	Success
Web Server	443	Success

Close Help

FIGURE 17 Port Status dialog box

The status options are as follows:

- Success—The port is listening or bound to the server.
- Failed—The port fails to listen or bind to the server.
- Disabled (FTP port only)—only displays when the FTP server is external. This is considered a normal status.

2. Click **Close**.

# License

---

**NOTE**

If your installation does not require a license key, the **License** dialog box does not display.

---

License keys are unique strings of alphanumeric characters that verify ownership of the Management application software as well as determine the maximum port count allowed or any additional features (such as Event Management) that you receive as part of the license.

---

**NOTE**

Enterprise edition can manage up to 9000 ports.

---

## Managed port count calculation

The managed port count is calculated using the following rules:

---

**NOTE**

If you exceed the maximum port count for your edition, software functionality is impacted and you must reduce the port count using the **Discovery Setup** dialog box or contact your storage vendor to purchase additional ports.

---

1. The switch port must be licensed.
2. The ports must belong to a currently monitored fabric.
3. ICL ports are not counted.
4. The port must be a physical port (for example, VE Ports are not counted the 4 Gbps Router, Extension Switch; however, the Gbit ports are counted).
5. Access Gateway ports are counted.
6. The ports from discovered Virtual Fabrics are counted.
7. The ports from managed Fabric OS and M-EOS switches are counted.
8. The ports from 'missing switches' are not counted.

## Entering the license key

A license key is required to run the application. The key specifies the expiration date of a trial license, as well as the number of ports allowed.

---

### NOTE

You are not required to enter a license key for a trial license. If you do not enter the license key during installation of Professional Plus or Enterprise editions, you can use the application, including all of its features, for a trial period of 75 days. At the termination of the trial period, a **License** dialog displays, where you must enter a license key.

---

---

### NOTE

You are not required to enter a license key for SMI Agent only installation. If you choose to the SMI Agent only option, when you open the Management application client, a **License** dialog displays, where you must enter a license key.

---

Before you enter the license key you must install the application. For step-by-step instructions, refer to “Installing the Application” in the *DCFM Installation Guide*.

1. Select **Help > License**.

The **License** dialog box displays

2. Choose from one of the following options:

- Enter the license key in the **License Key** field.

The **License Key** field is not case-sensitive.

- Browse to the license file.

3. Click **Update** to extract the new license information.

Review the new information in the **License** dialog box fields.

4. Click **OK** to set the new license on the Server.

A message displays. Click **OK** to close the message and log off the client. To see the changes to the client, open the application and log in using the instructions in “[Logging into a server](#)” on page 17.

## Upgrading the application

The quickest and simplest method of moving from one edition to another is to enter the new license information on the **License** dialog box. The following table list the available upgrade paths:

Current Software Release	To Software Release
Professional Plus trial	Professional Plus edition Enterprise edition
Professional Plus edition	Enterprise edition
Enterprise trial	Enterprise edition

1. Select **Help > License**.

The **License** dialog box displays.

2. Enter the license key (on the Key Certificate) in the **License Key** field and click **Update**.
3. Click **OK** on the message.

The Client closes after updating the license successfully. Restart the Server, Client and Server Management Console for the changes to take effect.

4. Open the application (double-click the desktop icon or open from the **Start** menu).

The **Log In** dialog box displays.

5. Enter your user name and password.

The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

6. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
7. Click **Login**.
8. Click **OK** on the Login Banner.

## Installing a patch

The patch installer enables you to update the Management application between releases. Each patch installer includes the previous patches within a specific release. For example, patch F (10.4.0f) includes the upgrades in the patch installers for A (10.4.0a) through E (10.4.0e).

To install a patch, complete the following steps.

1. Stop all services by completing the following steps.
  - a. Launch the Server Console.
  - b. Click the **Services** tab.
  - c. Click **Stop** to stop all services.

2. Go to the *Install\_Home/bin* directory.

3. Execute the patch file for your operating system:

`patch.bat` (Windows)

`patch.sh` (UNIX)

The **Upgrade** dialog box displays.

4. Browse to the patch file.

The patch zip file uses the following naming convention:

*Management\_Application\_Name-Major\_Version-Minor\_Version-Revision\_Number-patch-Patch\_Version.zip* (for example *Management\_Application\_Name-10-4-0-patch-a.zip*).

# 1 Uninstalling a patch

## 5. Click **Upgrade**.

If the patch process is interrupted (for example, loss of power), you must restart the patch process.

The patch installer performs the following functions:

- Extracts patch files to the *Install\_Home* folder.
- Creates a back up (zip) of the original files to be updated and copies the zip file to the *Install\_Home\patch-backup* directory. For example, *Install\_Home\patch-backup\Management\_Application\_Name-10-4-0-patch-a.zip*.
- Generates a patch log.
- Updates the conf file (*Install\_Home\conf\patch.conf*) to include the patch version applied and patch created date.
- Updates the patch version in the **About** dialog box (Select **Help > About** in the main window).

## 6. Start all services by completing the following steps.

- a. Launch the Server Console.
- b. Click the **Services** tab.
- c. Click **Start** to start all services.

## Uninstalling a patch

Note that only one set of back up files are retained which enables you revert back to the previous version. You can only revert back one version. For example:

- If you upgrade from patch A to patch B, you can revert back to patch A.
- If you upgrade from patch A to patch B to patch C then to patch F, you can only revert back to patch C.

To uninstall a patch, complete the following steps.

## 1. Stop all services by completing the following steps.

- a. Launch the Server Console.
- b. Click the **Services** tab.
- c. Click **Stop** to stop all services.

## 2. Go to the *Install\_Home/patch-backup* directory.

## 3. Extract the patch zip file (for example, *Management\_Application\_Name-10-4-0-patch-a.zip*).

## 4. Open the *restore.xml* file from the extracted files.

The artifacts (jar files, war files, and so on) you need to replace display as separate file tags in the *restore.xml* file. The location of each artifact in the extracted folder is detailed in the *src* value under each file tag.

## 5. Go to the location of the first artifact (as shown in the *src* value under the file tag).

## 6. Copy the artifact from the extracted folder to the source folder in the *Install\_Home/patch-backup* directory.

## 7. Repeat step 5 and 6 for all artifacts listed in the *restore.xml* folder.

8. Go to the *Install\_Home/conf* directory.
9. Open the *version.properties* file in a text editor.
10. Change the patch version (*patch.version*) value to the reverted patch (for example, if you are reverting from patch F to patch C then *patch.version = c*).  
  
If the previous version is the initial version (no patches), change the patch version value to none (for example, *patch.version = None*).
11. Go to the *Install\_Home/patch-backup/conf* directory.
12. Copy the *patch.conf* file in this directory to the *Install\_Home/conf* directory.  
  
If the previous version is the initial version (no patches), delete the *patch.conf* file in the *Install\_Home/conf* directory.
13. Start all services by completing the following steps.
  - a. Launch the Server Console.
  - b. Click the **Services** tab.
  - c. Click **Start** to start all services.

## Feature-to-firmware requirements

Use the following table to determine whether the Management application features are only available with a specific version of the Fabric OS firmware, M-EOS firmware, or both, as well as if there are specific licensing requirements.

Feature	Fabric OS	M-EOS
Access Gateway (AG)	AG connected to Fabric OS devices requires firmware 6.1.1 or later.	AG connected to M-EOS devices requires firmware 9.9.2 or later.
Call Home	Requires Fabric OS 5.2 or later for supportSave. Requires Fabric Watch license for SNMP traps.	Requires M-EOS and M-EOSn 9.6.X or later.
Discovery	Requires Fabric OS 5.0 or later for the seed switch in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later for the seed switch in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS 9.9.2 or later for the seed switch in a pure M-EOS fabric. Requires M-EOS and M-EOSn 9.6.X or later for discovery.
Encryption	Requires Fabric OS 6.1.1_enc.	Not available.
Enhanced Group Management	Requires Enhanced Group Management license.	Not available.
Fault Management	Requires Fabric OS 4.4 or later for SNMP traps	Requires M-EOS and M-EOSn 9.6.X or later.
Fabric Binding	Requires Fabric OS 5.2 or later in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS and M-EOSn 9.6.X or later.
FCIP Management	Requires Fabric OS 5.1 or later to modify. Requires Fabric OS 5.3 or later for FCIP tunnels. Requires FCIP license. Requires Fabric OS 6.0 or later to enable the FICON Emulation tab on the FCIP Tunnel Advanced Settings dialog box.	Not available.

# 1 Feature-to-firmware requirements

Feature	Fabric OS	M-EOS
FICON	Requires Fabric OS 5.2 or later for cascaded FICON. Requires Fabric OS 6.0 or later for advanced FICON. Requires Fabric OS 6.1.1 or later to configure multiple Prohibit Dynamic Connectivity Mask (PDCM) matrices. Requires FICON CUP license to allow CUP management features.	Only supports cascaded FICON configuration for mixed fabrics.
Firmware Management	Requires Fabric OS 5.0 or later. Requires Fabric OS 6.1.1 or later on 8G devices. Requires Enhanced Group Management license to perform group actions.	Firmware download is only available through the Element Manager.
High Integrity Fabric	Requires Fabric OS 5.2 or later in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS and M-EOSn 9.6.X or later.
Meta SAN	Requires Fabric OS 5.2 or later for FC router and router domain ID configuration. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric. Requires Integrated Routing license.	Not available.
Performance	Requires Fabric OS 5.0 or later for FC_ports, end-to-end monitors, and marching ants. Requires Fabric OS 5.3 or later for GE_ports and FCIP tunnels. Requires Fabric OS 6.2 or later for Top Talkers. Requires Advanced Performance Monitoring (APM) license for End-to-end Monitoring and Top Talkers. Requires Enhanced Group Management license for Hlistorical graphs and tables. Requires Fabric Watch license for Performance thresholds.	Requires M-EOS and M-EOSn 9.6.X or later for FC_ports and marching ants.
Port Fencing	Requires Fabric OS 6.2 or later.	Requires M-EOS and M-EOSn 9.6.X or later.
Security Management	Requires Fabric OS 5.2 and later for SCC Policy. Requires Fabric OS 5.2 and later for DCC Policy. Requires Fabric OS 5.3 and later for IP Filter Policy. Requires Fabric OS 6.0 and later for AD/LDAP Server Configuration. Requires Fabric OS 5.0 and later for RADIUS Server Configuration.	Not available.
Technical Support Data Collection	Requires Fabric OS 5.2 or later.	Data collection support is only available through the Element Manager.
Troubleshooting and Diagnostics	Requires Fabric OS 5.2 or later.	Not available.

Feature	Fabric OS	M-EOS
Virtual Fabrics	Requires at least one Virtual Fabrics-enabled physical chassis running Fabric OS 6.2 or later.	Virtual Fabric configuration is only available through the Element Manager.
Zoning	Requires Fabric OS 5.0 or later for pure Fabric OS fabrics. Requires Fabric OS 6.0 or later for McDATA Fabric Mode. Requires Adaptive Networking license for Quality of Service zones.	Requires M-EOS and M-EOSn 9.6.X or later for a pure M-EOS fabric and Mixed Fabrics in Interopmode 3.

## Accessibility features for the Management application

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features in the Management application:

- Keyboard shortcuts
- Look and Feel

### Keyboard shortcuts

You can use the keystrokes shown in the table below to perform common functions.

#### NOTE

To open a menu using keystrokes, press ALT plus the underlined letter. To open a submenu, open the menu, then press the key for the underlined letter (SHIFT plus letter for capitals) of the submenu option.

Menu Item or Function	Keyboard Shortcut
All Panels	F12
Collapse	CTRL + L
Command Tool	SHIFT + F4
Connectivity Map	F7
Copy	CTRL + C
Cut	CTRL + X
Delete	Delete
Delete All	CTRL +Delete
Help	F1
Internet Explorer	SHIFT + F2
Master Log	F5
FireFox	SHIFT + F1
Paste	CTRL + V
Product List	F9

# 1 Look and Feel

Menu Item or Function	Keyboard Shortcut
Properties	Alt-Enter
Select All	CTRL + A
Show Ports	F4
SSH	Shift-F5
View Utilization	CTRL + U
Zoom In	CTRL + NumPad+
Zoom Out	CTRL + NumPad-

## Look and Feel

You can configure the Management application to mimic your system settings as well as define the size of the font.

‘Look’ refers to the appearance of graphical user interface widgets and ‘feel’ refers to the way the widgets behave.

The Management application currently uses the ‘*Management\_Application* Default Look and Feel’ for some of the components (for example, Layout, Minimap, and so on) and the “Java Metal Look and Feel” for others.

### *Setting the look and feel*

#### NOTE

Setting the look and feel is only supported on Windows systems.

The following table details the Management application components that change when you set the look and feel as well as those components that do not change.

Components Affected	Components Not Affected
All Java native components with Metal Look And Feel are affected.	The Connectivity map does not change when devices are present. You must change the theme using the map display settings ( <b>View &gt; Map Display</b> ).
The Menu bar, Tool bar, Status bar, as well as all tables and dialog boxes are affected.	All icons and images are not affected.
Layout is affected only when it is empty.	The Minimap is not affected.

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **Look and Feel** in the **Category** list.

3. Choose from one of the following options:
  - Select **Default** to configure the look and feel back to the Management application defaults.
  - Select **System** to configure the Management application to have the look and feel of your system.

This changes the look and feel for the components that use 'Java Metal Look and Feel'. For example, if you have your system display color scheme set to 'High Contrast #1', then the Management application will be set to 'High Contrast #1'. Font size of the components is not affected by theme changes.
4. Click **Apply** or **OK** to save your work.
5. Click **OK** on the message.

---

**NOTE**

Changes do not take affect until after you restart the client.

---

### *Changing the font size*

The **Options** dialog box enables you to change the font size for all components including the Connectivity map of the Management application interface.

Font size changes proportionately in relation to the system resolution. For example, if the system resolution is 1024 x 768, the default font size would be 8 and large font size would be 10.

1. Select **Server > Options**.

The **Options** dialog box displays.
2. Select **Look and Feel** in the **Category** list.
3. Select one of the following options from the **Font Size** list:
  - Select **Default** to return to the default font size.
  - Select **Small** to change the font to a smaller font size.
  - Select **Large** to change the font to a larger font size.

---

**NOTE**

Changing the font size to **Large** may cause the interface components (for example, text and button labels) to display incorrectly.

---

4. Click **Apply** or **OK** to save your work.
5. Click **OK** on the message.

---

**NOTE**

Changes do not take affect until after you restart the client.

---

# 1 Look and Feel

# Discovery

---

## In this chapter

• Fabric discovery overview . . . . .	35
• Host discovery . . . . .	42
• Viewing the discovery state. . . . .	48
• Fabric monitoring. . . . .	52
• Seed switch . . . . .	53

## Fabric discovery overview

Discovery is the process by which the Management application contacts the devices in your SAN. When you configure discovery, the application discovers products connected to the SAN. The application illustrates each product and its connections on the Connectivity Map (topology).

When you discover a fabric, the Management application checks to confirm that the seed switch is running a supported Fabric OS or M-EOS version in the fabric, and if it is not, the Management application prompts you to select a new seed switch.

---

### NOTE

Discovery of a Secure Fabric OS fabric in strict mode is not supported.

---

For a Fabric OS fabric, the seed switch must be the primary Fabric Configuration Server (FCS). If you use a non-primary FCS to discover the fabric, the Management application displays an error and will not allow the discovery to proceed. If the Management application has already discovered the fabric, but afterward you create the FCS policy and the seed switch is not a primary FCS, an event is generated during the next poll.

The Management application cannot discover a fabric that is in the process of actively configuring to form a fabric. Wait until the fabric is formed and stable, then re-attempt the fabric discovery.

After fabric discovery successfully completes, all clients are updated to display the newly discovered fabric.

During fabric discovery, if you have defined IPv6 IP addresses for the switch, the Management application remembers the IP address only. If the switch has a DNS name that you have defined, the Management application can remember the DNS name and use that.

## FCS policy and seed switches

The Management application requires that the seed switch is the primary Fabric Content Service (FCS) switch at the time of discovery.

Setting time on the fabric will set the time on the primary FCS switch, which will then distribute the changes to other switches.

When FCS Policy is defined, **ConfigDownload** is allowed only from the primary FCS switch, but Management application does not check at the time of download that the switch is the primary FCS Switch.

---

**NOTE**  
Switches running in Access Gateway mode cannot be used as the seed switch.

---

---

**NOTE**  
The Backbone Chassis cannot be used as a seed switch.

---

## Discovering fabrics

---

**NOTE**  
Fabric OS devices must be running Fabric OS 5.0 or later. M-EOS devices must be running M-EOS 9.6 or later.

---

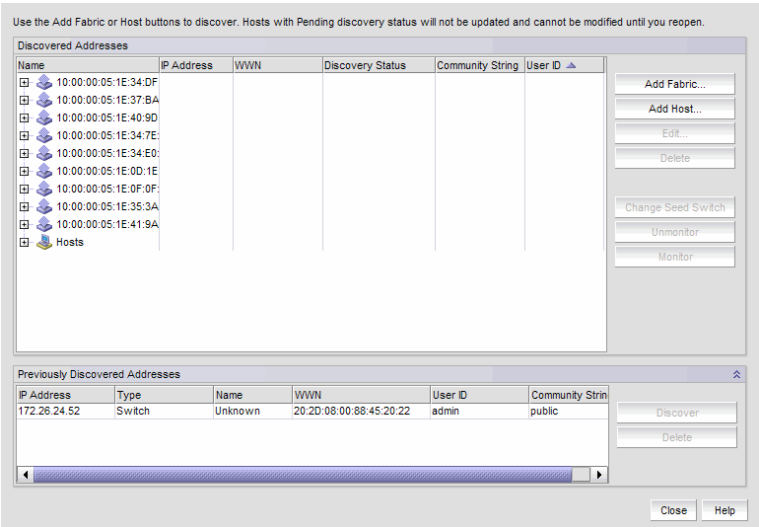
---

**NOTE**  
Only one copy of the application should be used to monitor and manage the same devices in a subnet.

---

To discover specific IP addresses or subnets, complete the following steps.

- 1. Select **Discover > Setup**.  
The **Discover Setup** dialog box displays.



**FIGURE 18**    Discover Setup dialog box

- Click **Add Fabric** to specify the IP addresses of the devices you want to discover.

The **Address Properties** dialog box displays.

**FIGURE 19** Address Properties dialog box (IP Address tab)

- Enter a name for the fabric in the **Fabric Name** field.
- Enter an IP address for a device in the **IP Address** field.

For seed switch requirements, refer to [“Seed switch requirements”](#) on page 54.

---

#### NOTE

The Backbone Chassis cannot be used as a seed switch.

---

For M-EOS devices, the Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the Operating System has IPv4 mode only or dual stack mode. The IPv6 format is valid when the Operating System has IPv6 mode only or dual stack mode.

If the firmware version is between M-EOS 9.6.X and 9.9.2, only the domain ID, WWN, and topology are obtained for fabric members. To manage other fabric members, you must enter specific IP addresses in the **Discover Setup** dialog box.

For Admin Domain (AD) discovery, Fabric OS switch must have Physical AD visibility.

For Virtual Fabric discovery device requirements, refer to [“Virtual Fabrics requirements”](#) on page 590.

To discover a Virtual Fabric device, you must have the following permissions:

- Switch user account with Chassis Admin role permission on the physical chassis.
- Switch and SNMP v3 user account with access rights to all logical switches (all Fabric IDs (1 - 128)).

For information about configuring permissions on a Fabric OS device, refer to the *Fabric OS Administrator's Guide*.

- (Fabric OS devices only) Enter the user ID and password for the switch in the **User ID** and **Password** fields.

6. Click the **SNMP** tab (Figure 20).

**FIGURE 20** Address Properties dialog box (SNMP - v1 tab)

7. Enter the duration (in seconds) after which the application times out in the **Time-out (sec)** field.
8. Enter the number of times to retry the process in the **Retries** field.
9. Select the SNMP version from the **SNMP Version** list.

- If you selected v1, continue with step 10.
- If you select v3, the SNMP tab displays the v3 required parameters. Go to step 14.

To discover a Fabric OS device (not virtual fabric-capable), you must provide the existing SNMP v3 username present in the switch.

To discover a Virtual Fabric device, you must configure SNMP v3 and your SNMP v3 user account must be defined as a Fabric OS switch user.

### NOTE

When you discovers Virtual Fabric-enabled switch with the SNMP v3 username “admin”, which is the same as the Fabric OS switch user, the Management application automatically creates an SNMP username “admin” in the switch by replacing the sixth username.

10. Specify the **Read** option by selecting **Default ‘public’** or **Custom**.
  11. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.
  12. Specify the **Write** option by selecting **Default ‘private’** or **Custom**.
  13. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.
- Go to step 21.

14. If you are configuring a 256-port director, select the **Configure for 256-Port\_Director\_Name** check box.

- If you selected **Configure for 256-Port\_Director\_Name**, go to step 18.
- If you did not select **Configure for 256-Port\_Director\_Name**, continue with step 15.

**FIGURE 21** Address Properties dialog box (SNMP Tab - v3)

15. Enter a user name in the **User Name** field.

16. Enter a context name in the **Context Name** field.

17. Select the authorization protocol in the **Auth Protocol** field.

18. Enter the authorization password in the **Auth Password** field.

- If you selected **Configure for 256-Port\_Director\_Name**, go to step 21.
- If you did not select **Configure for 256-Port\_Director\_Name**, continue with step 19.

19. Select the privacy protocol in the **Priv Protocol** field.

20. Enter the privacy password in the **Priv Password** field.

21. Click **OK** on the **Address Properties** dialog box.

If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays.

- Select the **Select** check box for each undiscovered seed switch to discover their fabrics.
- Click **OK** on the **Undiscovered Seed Switches** dialog box.

22. Repeat [step 2](#) through [step 21](#) for each fabric you want to discover.

23. Click **OK** on the **Discover Setup** dialog box.

## Configuring SNMP credentials

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Select an IP address from the **Available Addresses** table.

3. Click **Edit**.

The **Address Properties** dialog box displays.

4. Click the **SNMP** tab.

## 2 Configuring SNMP credentials

5. Select the SNMP version from the **SNMP Version** list.
  - If you selected v1, continue with step 6.
  - If you select v3, the **SNMP** tab displays the v3 required parameters. Go to step 10.  
To discover a Virtual Fabric device, you must configure SNMP v3 and your SNMP v3 user account must be defined as a Fabric OS switch user.
6. Specify the **Read** option by selecting **Default 'public'** or **Custom**.
7. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.
8. Specify the **Write** option by selecting **Default 'private'** or **Custom**.
9. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.  
Go to step 21.
10. If you are configuring a 256-Port director, select the **Configure for 256-Port\_Director\_Name** check box.
  - If you selected **Configure for 256-Port\_Director\_Name**, go to step 14.
  - If you did not select **Configure for 256-Port\_Director\_Name**, continue with step 11.

The image shows a screenshot of the 'Address Properties' dialog box with the 'SNMP' tab selected. The dialog has two tabs: 'IP Address' and 'SNMP'. Under the 'SNMP' tab, there are several fields: 'Target Port' (set to 161), 'Time-out (sec)' (set to 5), and 'Retries' (set to 3). Below these is the 'SNMP Version' dropdown menu, which is set to 'v3'. There is a checkbox labeled 'Configure for Intrepid 10K' which is currently unchecked. Below the checkbox are several text input fields: 'User Name', 'Context Name', 'Auth Password', and 'Priv Password'. There are also two dropdown menus: 'Auth Protocol' (set to '- None -') and 'Priv Protocol' (set to '- None -'). At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

**FIGURE 22** Address Properties dialog box (SNMP Tab - v3)

11. Enter a user name in the **User Name** field.
12. Enter a context name in the **Context Name** field.
13. Select the authorization protocol in the **Auth Protocol** field.
14. Enter the authorization password in the **Auth Password** field.
  - If you selected **Configure for 256-Port\_Director\_Name**, go to step 17.
  - If you did not select **Configure for 256-Port\_Director\_Name**, continue with step 15.
15. Select the privacy protocol in the **Priv Protocol** field.
16. Enter the privacy password in the **Priv Password** field.
17. Click **OK** on the **Address Properties** dialog box.

If the seed switch is not partitioned, continue with [step 18](#).

If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays.

- a. Select the **Select** check box for each undiscovered seed switch to discover their fabrics.
  - b. Click **OK** on the **Undiscovered Seed Switches** dialog box.
18. Click **OK** on the **Discover Setup** dialog box.

## Reverting to a default SNMP community string

1. Select **Discover > Setup**.  
The **Discover Setup** dialog box displays.
2. Select an IP address from the **Available Addresses** table.
3. Click **Edit**.  
The **Address Properties** dialog box displays.
4. Click the **SNMP** tab.
5. Click **Default 'public'** and **Default 'private.'**
6. Click **OK** on the **Address Properties** dialog box.
7. Click **OK** on the **Discover Setup** dialog box.

## Deleting a fabric

If you decide you no longer want the Management application to discover and monitor a specific fabric, you can delete it. Deleting a fabric also deletes the fabric data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a fabric, complete the following steps.

1. Select **Discovery > Setup**.  
The **Discover Setup** dialog box displays.
2. Select the fabric for which you want to delete from the **Discovered Addresses** table.
3. Click **Delete**.  
You are prompted to confirm that you want to delete the fabric.

# Host discovery

The Management application enables you to discover individual hosts, import a group of Host from a comma separated values (CSV) file, or import all hosts from discovered fabrics.

---

**NOTE**  
Host discovery requires HCM Agent 2.0 or later.

---



---

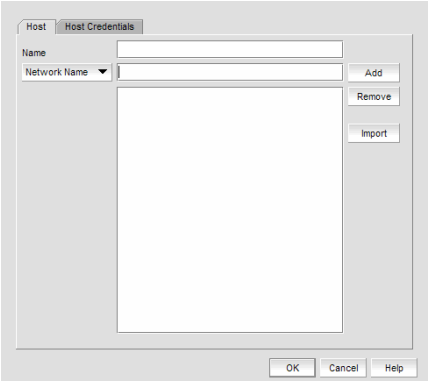
**NOTE**  
SMI and WMI discovery are not supported.

---

## Discovering Hosts by IP address or hostname

To discover a Host by IP address or hostname, complete the following steps.

1. Select **Discover > Setup**.  
The **Discover Setup** dialog box displays.
2. Click **Add Host**.  
The **Add Host Discovery** dialog box displays.



**FIGURE 23** Add Host Discovery dialog box - Host tab

3. Enter a discovery request name (such as, Manual 06/12/2009) in the **Name** field.
4. Select **Network Address** from the list.
5. Enter the IP address (IPv4 or IPv6 formats) or hostname in the **Network Address** field.
6. Click **Add**.  
The IP address or hostname of the Host displays in the text box.
7. Configure Host credentials, if necessary.  
To configure host credentials, refer to [“Configuring Brocade HBA credentials”](#) on page 45 or [“Configuring virtual machine credentials”](#) on page 46.
8. Repeat [step 5](#) through [step 7](#) for each Host you want to discover.

9. Click **OK** on the **Add Host Discovery** dialog box.

If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

10. Click **Close** on the **Discover Setup** dialog box.

## Importing Hosts from a CSV file

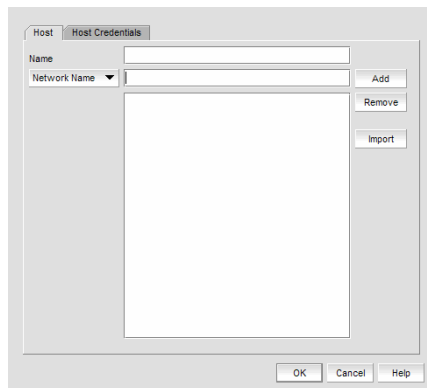
To discover Hosts by importing a CSV file, complete the following steps.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click **Add Host**.

The **Add Host Discovery** dialog box displays.



**FIGURE 24** Add Host Discovery dialog box - Host tab

3. Click **Import**.

The **Open** dialog box displays.

4. Browse to the CSV file location.

The CSV file must meet the following requirements:

- Comma separated IP address or host names
- No commas within the values
- No escaping supported

For example, XX.XX.XXX.XXX, XX.XX.X.XXX, computername.company.com

5. Click **Open**.

The CSV file is imported to the **Add Host** dialog box. During import, duplicate values are automatically dropped. When import is complete, the imported values display in the Host list text box. If the file cannot be imported, an error displays.

6. Verify the imported values in the **Host List** text box.

7. Configure Host credentials, if necessary.

To configure host credentials, refer to [“Configuring Brocade HBA credentials”](#) on page 45 or [“Configuring virtual machine credentials”](#) on page 46.

8. Click **OK** on the **Add Host Discovery** dialog box.

If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

9. Click **Close** on the **Discover Setup** dialog box.

### Importing Hosts from a Fabric

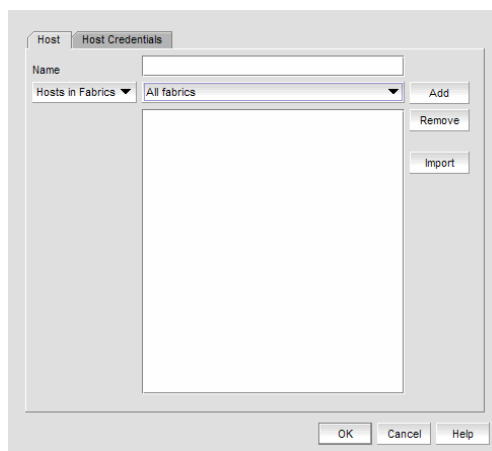
To discover a Host from a discovered fabric, complete the following steps.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click **Add Host**.

The **Add Host Discovery** dialog box displays.



**FIGURE 25** Add Host Discovery dialog box - Host tab

3. Enter a discovery request name (such as, MyFabric) in the **Name** field.
4. Select **Hosts in Fabric** from the list.
5. Select **All fabrics** or an individual fabric from the list.
6. Click **Add**.

All hosts which are part of a managed fabric and have a registered host name display in the text box. If no host with a registered host name exists, an error message displays. Click **OK** to close the error message.

7. Configure Host credentials, if necessary.

To configure host credentials, refer to [“Configuring Brocade HBA credentials”](#) on page 45 or [“Configuring virtual machine credentials”](#) on page 46.

8. Click **OK** on the **Add Host Discovery** dialog box.

If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

9. Click **Close** on the **Discover Setup** dialog box.

## Configuring Brocade HBA credentials

To configure credentials for a Brocade HBA, complete the following steps.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click **Add Host**.

The **Add Host Discovery** dialog box displays.

3. Discover a host.

To discover a host, refer to [“Discovering Hosts by IP address or hostname”](#) on page 42, [“Importing Hosts from a CSV file”](#) on page 43, or [“Importing Hosts from a Fabric”](#) on page 44.

4. Click the **Host Credentials** tab.

**FIGURE 26** Add Host Discovery dialog box - Host Credentials tab

5. Select the **Discover Brocade HBAs in the hosts** check box, if necessary.
6. Enter the HCM Agent port number in the **Brocade HBAs - Port** field if necessary.
7. Enter your username and password in the appropriate fields.
8. Click **OK** on the **Add Host Discovery** dialog box.

If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

9. Click **Close** on the **Discover Setup** dialog box.

### Configuring virtual machine credentials

To configure credentials for a virtual machine, complete the following steps.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click **Add Host**.

The **Add Host Discovery** dialog box displays.

3. Discover a host.

To discover a host, refer to [“Discovering Hosts by IP address or hostname”](#) on page 42, [“Importing Hosts from a CSV file”](#) on page 43, or [“Importing Hosts from a Fabric”](#) on page 44.

4. Click the **Host Credentials** tab.

**FIGURE 27** Add Host Discovery dialog box - Host Credentials tab

5. Select the **Discover Brocade HBAs in the hosts** check box, if necessary.
6. Enter the HCM Agent port number in the **Brocade HBAs - Port** field if necessary.
7. Enter your username and password in the appropriate fields.
8. Select the **Discover virtual machine information in the hosts** check box.
9. Enter the virtual machine port number in the **Brocade HBAs - Port** field if necessary.
10. Enter your username and password in the appropriate fields.
11. Click **OK** on the **Add Host Discovery** dialog box.

If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

A Host Group displays in **Discovered Addresses** table with pending status. To update the status from pending you must close and reopen the **Discover Setup** dialog box.

12. Click **Close** on the **Discover Setup** dialog box.

## Editing Host credentials

To edit Host credentials, complete the following steps.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Select the Host and click **Edit**.

The **Edit Host Discovery** dialog box displays.

The screenshot shows the 'Edit Host Discovery' dialog box. It is divided into two main sections: 'Brocade HBAs' and 'Virtual Machines'. Each section has a checkbox labeled 'Discover [Section Name] in the host' which is checked. Below each checkbox are three input fields: 'Port', 'User ID', and 'Password'. In the 'Brocade HBAs' section, the Port is 34568, User ID is admin, and Password is masked with dots. In the 'Virtual Machines' section, the Port is 443, User ID is admin, and Password is masked with dots. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

**FIGURE 28** Edit Host Discovery dialog box

3. To edit Brocade HBA credentials, select the **Discover Brocade HBAs in the hosts** check box, if necessary, and complete the following steps.
  - a. Enter the HCM Agent port number in the **Brocade HBAs - Port** field if necessary.
  - b. Enter your username and password in the appropriate fields.
4. To edit virtual machine credentials, select the **Discover virtual machine information in the hosts** check box, if necessary, and complete the following steps.
  - a. Enter the virtual machine port number in the **Brocade HBAs - Port** field if necessary.
  - b. Enter your username and password in the appropriate fields.
5. Click **OK** on the **Edit Host Discovery** dialog box.
 

If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.
6. Click **Close** on the **Discover Setup** dialog box.

## Removing a Host from Discovery

To remove a Host from discovery, complete the following steps.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Select the Host you want to remove from discovery.
3. Click **Delete**.
4. Click **OK** on the confirmation message.

The deleted host displays in the **Previously Discovered Addresses** table.

5. Click **Close** on the **Discover Setup** dialog box.

## Viewing the discovery state

The Management application enables you to view device status through the **Discover Setup** dialog box.

To view the discovery status of a device, complete the following steps.




1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Right-click a fabric and select **Expand All** to show all devices in the fabric.

The **Name** field displays the discovery status icons in front of the device name. The following table illustrates and describes the icons that indicate the current status of the discovered devices.

**TABLE 4** Discovery Status Icons

Icon	Description
	Displays when the fabric or host is managed and the management status is okay.
	Displays when the fabric is managed and the switch management status is not okay.
	Displays when the fabric or host is not managed.

The **Discovery Status** field details the actual status message text, which varies depending on the situation. The following are samples of actual status messages:

- Discovered: Seed Switch: Not registered for SNMP Traps
- Discovered: Seed Switch: Not Manageable: Not registered for SNMP Traps
- Discovered: Current seed switch is not recommended. Change Seed Switch. : Seed Switch: Not registered for SNMP Traps

- New Discovery Pending
- Created host structure differs from discovered host; Discovery ignored
- Brocade HBA Discovery Failed: HCM Agent connection failed
- HCM Agent collection failed

## Troubleshooting discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

1. Verify IP connectivity by issuing a ping command to the switch.
  - a. Open the command prompt.
  - b. From the Server, type `ping Switch_IP_Address`.
2. Enter the IP address of the device in a browser to verify the SNMP settings.

For example, `http://10.1.1.11`.

### M-EOSn discovery troubleshooting

The following section states a possible issue and the recommended solution for M-EOSn discovery errors.

Problem	Resolution
<p>M-EOS seed switch discovery is not supported using SNMPv3 on the following devices:</p> <ul style="list-style-type: none"> <li>• 32-Port, 2 Gbps Switch</li> <li>• 16-Port, 4 Gbps Fabric Switch</li> <li>• 24-Port Fabric Switch</li> <li>• 32-Port, 4 Gbps Switch</li> <li>• 140-Port Director</li> </ul>	<p>Discover the device using SNMP v1.</p> <p>To configure SNMP v3 and manage the device, complete the following steps.</p> <ol style="list-style-type: none"> <li>1 Select <b>Discover &gt; Setup</b>. The <b>Discover Setup</b> dialog box displays.</li> <li>2 Select an IP address from the <b>Available Addresses</b> table.</li> <li>3 Click <b>Edit</b>. The <b>Address Properties</b> dialog box displays.</li> <li>4 Click the <b>SNMP</b> tab.</li> <li>5 Select the v3 from the <b>SNMP Version</b> list.</li> <li>6 If you are configuring a 256-Port director, select the <b>Configure for 256-Port_Director_Name</b> check box. <ul style="list-style-type: none"> <li>• If you selected <b>Configure for 256-Port_Director_Name</b>, go to step 10.</li> <li>• If you did not select <b>Configure for 256-Port_Director_Name</b>, continue with step 7.</li> </ul> </li> <li>7 Enter a user name in the <b>User Name</b> field.</li> <li>8 Enter a context name in the <b>Context Name</b> field.</li> <li>9 Select the authorization protocol in the <b>Auth Protocol</b> field.</li> <li>10 Enter the authorization password in the <b>Auth Password</b> field. <ul style="list-style-type: none"> <li>• If you selected <b>Configure for 256-Port_Director_Name</b>, go to step 13.</li> <li>• If you did not select <b>Configure for 256-Port_Director_Name</b>, continue with step 11.</li> </ul> </li> <li>11 Select the privacy protocol in the <b>Priv Protocol</b> field.</li> <li>12 Enter the privacy password in the <b>Priv Password</b> field.</li> <li>13 Click <b>OK</b> on the <b>Address Properties</b> dialog box. If the seed switch is not partitioned, continue with <a href="#">step 14</a>. If the seed switch is partitioned, the <b>Undiscovered Seed Switches</b> dialog box displays. <ol style="list-style-type: none"> <li>a. Select the <b>Select</b> check box for each undiscovered seed switch to discover their fabrics.</li> <li>b. Click <b>OK</b> on the <b>Undiscovered Seed Switches</b> dialog box.</li> </ol> </li> <li>14 Click <b>OK</b> on the <b>Discover Setup</b> dialog box.</li> </ol>
<p>If a fabric is formed with a M-EOSn 256-Port Director in dual IP address mode and then dual mode is disabled, the Management application cannot discover the 256-Port Director.</p>	<p>Rediscover the fabric.</p>

## Virtual Fabric discovery troubleshooting

The following section state possible issues and the recommended solutions for Virtual Fabric discovery errors.

Problem	Resolution
<p>At the time of discovery, the seed switch is Virtual Fabric-enabled; however, the user does not have Chassis Admin role for the seed switch.</p> <p>At the time of discovery, the user does not have the Chassis Admin role for all other switches in the fabric.</p> <p>After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, the user does not have Chassis Admin role.</p>	<p>Make sure the user account has Chassis Admin role on the Fabric OS device.</p>
<p>At the time of discovery, the seed switch is Virtual Fabric-enabled; however, the user does not have access to all possible logical switches (access to all possible Fabric IDs 1 - 128).</p> <p>At the time of discovery, the user does not have access to all possible logical switches for all other devices in the fabric.</p> <p>After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, the user does not have access to all possible logical switches.</p>	<p>Make sure the user account has access rights to all logical switches (access to all possible Fabric IDs 1 - 128) on the Fabric OS device.</p>
<p>At the time of discovery, SNMP v3 is not configured.</p> <p>At the time of discovery, SNMP v3 is not configured for all other switches in the fabric.</p> <p>After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, SNMP v3 is not configured</p>	<p>Configure the SNMP v3 information for the Virtual Fabric-enabled device.</p>
<p>At the time of discovery or fabric refresh, the SNMP v3 user account does not have the Chassis Admin role.</p>	<p>Make sure the SNMP v3 user account has the Chassis Admin role on the Fabric OS device.</p>
<p>At the time of discovery or refresh, the SNMP v3 user account does not have access to all possible logical switches (access to all possible Fabric IDs 1 - 128).</p> <p>This access is required to obtain performance statistics from all logical switches.</p>	<p>Make sure the SNMP v3 user account has access rights to all logical switches (access to all possible Fabric IDs 1 - 128) on the Fabric OS device.</p>
<p>At the time of discovery or fabric refresh, the SNMP v3 user account does not have a matching Fabric OS switch user account.</p> <p>This is required to obtain performance statistics from all logical switches.</p>	<p>Make sure the SNMP v3 user account is also defined as a Fabric OS switch user.</p>
<p>At the time of fabric refresh, the physical chassis is reachable; however, a previously discovered logical switch is not reachable.</p>	<p>The logical switch has been deleted or the Fabric ID was changed.</p> <p>To find a logical switch, right-click the physical chassis within the <b>Chassis Group</b> in the <b>Product List</b> and select <b>Logical Switches</b>.</p> <p>All logical switches on the selected physical chassis display in a list.</p>

# Fabric monitoring

**NOTE**  
Monitoring is not supported on Hosts. The upper limit to the number of HBA and CNA ports that can be monitored at the same time is 32. The same upper limit applies if switch ports and HBA ports are combined. You can select switch ports and adapter ports from a maximum of ten devices.

Fabric monitoring enables discovery of and data collection for the specified fabric and all associated devices. The Management application enables you to view fabric monitoring status through the **Discover Setup** dialog box. The following table illustrates and describes the icons that indicate the current status of the discovered fabrics.

**TABLE 5** Monitor Icons




Icon	Description
	Displays when the fabric is managed and the switch management status is okay.
	Displays when the fabric is managed and the switch management status is not okay.
	Displays when the fabric is not managed.

Table 6 details the default and minimum monitoring intervals used to query the monitored switches:

**TABLE 6** Monitor Intervals

SAN Size	Default	Minimum
Small	120 seconds (2 minutes)	60 seconds (1 minute)
Medium	900 seconds (15 minutes)	120 seconds (2 minutes)
Large	1800 seconds (30 minutes)	180 seconds (3 minutes)

To change the monitoring interval, refer to [“Configuring asset polling”](#) on page 99.

## Monitoring discovered fabrics

**NOTE**  
Monitoring is not supported on Hosts.

To monitor a fabric and all associated devices, complete the following steps.

1. Select **Discovery > Setup**.  
The **Discover Setup** dialog box displays.
2. Select the fabric you want to monitor from the **Discovered Addresses** table.

3. Click **Monitor**.

The monitor function fails if the fabric has user-defined Admin Domains created or if the fabric is merged with another fabric already in the monitored state.

4. Click **OK**.

## Stop monitoring of a discovered fabric

---

### NOTE

Monitoring is not supported on Hosts.

---

When you stop monitoring of a fabric, you stop discovery of and data collection for the specified fabric and all associated devices.

To stop monitoring a fabric and all associated devices, complete the following steps.

1. Select **Discovery > Setup**.

The **Discover Setup** dialog box displays.

2. Select the fabric you want to stop monitoring from the **Discovered Addresses** table.
3. Click **Unmonitor**.
4. Click **OK**.

## Seed switch

The seed switch must be running a supported Fabric OS or M-EOS version and must be HTTP-reachable.

Sometimes, the seed switch is auto-selected, such as when a fabric segments or when two fabrics merge. Other times, you are prompted (an event is triggered) to change the seed switch, such as in the following cases:

- If, during fabric discovery, the Management application detects that the seed switch is not running a supported version, you are prompted to change the seed switch.
- When one or more switches join the fabric or if the switch firmware is changed on any of the switches in the fabric, the Management application checks to make sure that the seed switch is still running a supported version. If it is not, then you are prompted to either upgrade the firmware on the seed switch or to change the seed switch to a switch running a supported firmware.

If a fabric of switches running only Fabric OS 5.X or later is created due to segmentation, the Management application continues to monitor that fabric, but if any switch with a later Fabric OS version joins the fabric, an event is triggered informing you that the seed switch is not running the latest firmware and you should change to the seed switch running the highest firmware.

---

### ATTENTION

If a seed switch is segmented or merged, historical data such as offline zone DB, profile and reports, and Firmware Download Profile can be lost. Segmentation of a seed switch does not result in formation of a new fabric. If a merge occurs, the historical data is lost only from the second fabric.

---

You can change the seed switch as long as the following conditions are met:

- The new seed switch is HTTP-reachable from the Management application.
- The new seed switch is a primary FCS.
- The new seed switch is running the latest Fabric OS or M-EOS version in the fabric.

This operation preserves historical and configuration data, such as performance monitoring and user-customized data for the selected fabric.

---

### ATTENTION

If the seed switch firmware is downgraded from Fabric OS 5.2.X to an earlier version, then all RBAC-related data is discarded from the Management application.

---

If, during the seed switch change, the fabric is deleted, but the rediscovery operation fails (for example, if the new seed switch becomes unreachable using HTTP), then you must rediscover the fabric again. If you rediscover the fabric using a switch that was present in the fabric before the change seed switch operation was performed, then all of the historical and configuration data is restored to the rediscovered fabric. If you rediscover the fabric using a switch that was added to the fabric after the fabric was deleted, then the historical and configuration data is lost.

If multiple users try to change the seed switch of the same fabric simultaneously, only the first change seed switch request is executed; subsequent requests that are initiated before the first request completes will fail.

If another user changes the seed switch of a fabric you are monitoring, and if you have provided login credentials for only that seed switch in the fabric, then you lose connection to the seed switch.

## Seed switch requirements

Depending on your environment, you must meet the following hardware and firmware version requirements for seed switches.

Fabric OS devices:

- For Fabric OS only fabrics, the seed switch must be running Fabric OS 5.0 or later.
- For mixed fabrics (Fabric OS and M-EOS), the seed switch must be running Fabric OS 6.0 or later.

For a complete list of all supported Fabric OS hardware, refer to [“Supported hardware and software”](#) on page xxviii.

M-EOS devices:

- For pure M-EOS fabrics, the seed switch must be running M-EOS 9.6.X or later.

If the firmware version is between M-EOS 9.6.X and 9.9.2, only the domain ID, WWN, and topology are obtained for fabric members. To manage other fabric members, you must enter specific IP addresses in the **Discover Setup** dialog box.

If the firmware version is M-EOS 9.9.2 or later, discovery obtains all fabric member information for all fabric members. Fabric member information includes Domain ID, WWN, IP address (IPv4 and IPv6), Firmware Version, Model, and Vendor Name. The following M-EOS devices are both seed switch-capable and allow fabric member information collection:

- 32-Port, 4 Gbps Switch
- 16-Port, 4 Gbps Switch

- 140-Port Director
- 256-Port Director

The following M-EOS devices are seed switch-capable; however, they do not obtain fabric member information:

- 16-Port, 1 Gbps and 2 Gbps Switch
- 32-Port, 1 Gbps and 2 Gbps Switch
- 24-Port, 2 Gbps Switch
- 64-Port Director

## Seed switch failover

The Management application collects fabric-wide data (such as, fabric membership, connectivity, name server information, zoning, and so on) using the seed switch. Therefore when a seed switch becomes unreachable or there is no valid seed switch, the fabric becomes unmanageable.

When the seed switch cannot be reached for three consecutive fabric refresh cycles, the Management application looks for another valid seed switch in the fabric, verifies that it can be reached, and has valid credentials. If the seed switch meets this criteria, the Management application automatically fails over to the recommended seed switch.

Note that it is possible that auto-failover may occur to a seed switch not running the latest firmware version. In this instance, any functionality which has a direct dependency on the firmware version of the seed switch is affected and restricted by the failover seed switch capabilities.

Seed switch failover to a M-EOS switch is supported in a Mixed fabric with following restrictions:

- In Interop Mode 2 Fabrics, Defined Zone information is lost and the Management application cannot push the defined zone configuration to the switch because the M-EOS device is a seed switch.
- Dynamic updates do not occur when an end device is connected or removed from Fabric OS switch. Updates only occur during the asset polling cycle. The asset polling cycle defaults are based on SAN size (Small – 2 minutes, Medium – 15 minutes, Large – 30 minutes).
- If the firmware version is M-EOS 9.9.2 or later, discovery obtains all fabric member information for all fabric members. Fabric member information includes Domain ID, WWN, IP address (IPv4 and IPv6), Firmware Version, Model, and Vendor Name. The following M-EOS devices are both seed switch-capable and allow fabric member information collection:
  - 32-Port, 4 Gbps Switch
  - 16-Port, 4 Gbps Switch
  - 140-Port Director
  - 256-Port Director

The following M-EOS devices are seed switch-capable; however, they do not obtain fabric member information:

- 16-Port, 1 Gbps and 2 Gbps Switch
- 32-Port, 1 Gbps and 2 Gbps Switch
- 24-Port, 2 Gbps Switch
- 64-Port Director

## 2 Changing the seed switch

- Updates to Fabric OS switches (such as, Virtual Fabrics, FCR, Admin Domain, Switch Name and so on) do not occur.
- If the M-EOS switch is not seed switch capable and a switch joins the fabric, the IP address displays as '0.0.0.0'. You must manually edit the IP Address from the **Discover Setup** dialog box to manage the switch.
- Updates to firmware version and IP address of existing members do not occur.
- After failover to M-EOS switch occurs, if the Fabric OS switch becomes reachable again the Management application does not failover automatically to the Fabric OS switch. The seed switch status updates to "Current Seed switch is not recommended" in **Discover Setup** dialog box. You must manually change the seed switch to the Fabric OS switch using the **Change Seed Switch** dialog box. For more information, refer to "[Changing the seed switch](#)" on page 56.

### Changing the seed switch

When you change the seed switch for a fabric, the Management application performs the following checks in the order they are listed:

- Identifies all switches and removes those running unsupported firmware version.
- Identifies which of the remaining switches are running the latest firmware versions.
- Filters out those switches that are not reachable.
- Identifies which switches are Virtual Fabric-enabled switches (Fabric OS only).  
If there are Virtual Fabric-enabled switches, the Management application only uses these switches as recommended seed switches. If there are no Virtual Fabric-enabled switches, continue with the next check.
- Identifies which switches are Virtual Fabric-capable devices (Fabric OS only).  
If there are Virtual Fabric-capable switches, the Management application only uses these switches as recommended seed switches. If there are no Virtual Fabric-capable switches, the Management application uses the list from the second check.

To change the seed switch, complete the following steps.

1. Select **Discovery > Setup**.  
The **Discover Setup** dialog box displays.
2. Select the fabric for which you want to change the seed switch from the **Discovered Addresses** table.  
If a device joins or merges with a fabric and fabric tracking is active, you must accept changes to the fabric before the new devices display in the **Change Seed Switch** dialog box. For more information about fabric tracking, refer to "[Fabric tracking](#)" on page 102.
3. Click **Change Seed Switch**.  
If the fabric contains other switches that are running the latest version and are also HTTP-reachable from the Management application, the **Change Seed Switch** dialog box appears. Otherwise, a message displays that you cannot change the seed switch.

4. Select a switch to be the new seed switch from the **Change Seed Switch** dialog box.

You can select only one switch. Only switches that are running the latest Fabric OS version in the fabric are displayed. The current seed switch is not displayed in this list.

5. Click **OK**.

If you are not already logged in to the seed switch, the **Fabric Login** dialog box displays.

If you are successfully authenticated, the fabric is deleted from the Management application without purging historical data, and the same fabric is rediscovered with the new seed switch.

6. Click **OK**.

## 2 Changing the seed switch

# Application Configuration

---

## In this chapter

• Data backup .....	59
• Data restore .....	67
• Display .....	68
• End node display .....	70
• Ethernet events .....	71
• Event storage .....	72
• Flyovers .....	73
• Names .....	76
• Security .....	84
• Software Configuration .....	87

## Data backup

The Management application helps you to protect your data by backing it up automatically. The data can then be restored, as necessary.

---

### NOTE

Backing up data takes some time. It is possible that, in a disaster recovery situation, configuration changes made after the last backup interval will be missing from the backup.

---

The Management application allows you to view the backup status at a glance, initiate immediate backup, enable or disable automatic backup, reconfigure the backup directory, interval, and start time, and retrieve backup events.

## What is backed up?

The data is backed up to the following directories:

- Backup\databases — contains database and log files.
- Backup\data — contains M-EOS switches Element Manager data files (including Dump files, Data collection progress files, Director/Switch firmware files FAF files, Switch technical supportSave, and Switch backup files) and Fabric OS miscellaneous files.
- Backup\conf — contains the Management application configuration files.
- Backup\cimom — contains the SMIA configuration files.

### Management server backup

There are three options for backing up data to the management server:

- Configuring backup to a writable CD
- Configuring backup to a hard drive
- Configuring backup to a network drive

The Management Server is backed up to a rewritable (CD-RW) compact disk by default. Make sure you have a CD-RW disk in the CD recorder drive to ensure that backup can occur. Critical information from the Management application is automatically backed up to the CD-RW when the data directory contents change or when you restart the Management application.

Note that backing up to CD is not the recommended method. The usable capacity of a CD is approximately 700 MB and needs to be replaced when full. Also, CD media has a limited number of re-writes before the medium is exhausted, and write errors occur. It is recommended that you configure the backup system to target a hard drive or a network drive as described in the procedures below.

#### *Back up directory structure overview*

The Management server backs up data to two alternate folders. For example, if the backup directory location is D:\Backup, the backup service alternates between two backup directories, D:\Backup and D:\BackupAlt. The current backup is always D:\Backup and contains a complete backup of the system. The older backup is always D:\BackupAlt.

If a backup cycle fails, the cause is usually a full CD-RW. When the backup cycle fails, there may only be one directory, D:\Backup. There may also be a D:\BackupTemp directory. Ignore this directory because it may be incomplete.

## Configuring backup to a writable CD

### NOTE

This is not recommended on a permanent basis. CDs have a limited life, and may only last a month. An error message occurs if your Management application can no longer back up to the disc.

To configure the backup function to a writable CD, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays (Figure 29).

This option allows you to configure backup settings. Backup is a service process that periodically copies and stores application files to an output directory. The output directory is relative to the server and must use a network share format to support backup to the network. If you use a network path as the output directory, you must add network credentials as well.

☒ Enable Backup

☒ Include FTP Root Directory

☒ Include Technical Support Directory

☒ Include Upload Failure Data capture Directory

Next Backup Start Time: 13 Hours 34 Minutes

Backup Interval: 24 Hours [Backup Now]

Output Directory: D:/Backup [Browse...]

Network Drive Credentials

Domain Workgroup: [ ]

User Name: [ ]

Password: [ ]

[OK] [Cancel] [Apply] [Help]

**FIGURE 29** Options dialog box (Backup option)

2. Select **Backup** in the **Category** list.

The currently defined directory displays in the **Backup Output Directory** field.

3. Select the **Enable Backup** check box, if necessary.
4. Choose one or more of the following options:
  - Select the **Include FTP Root Directory** check box.  
If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.
  - Select the **Include Technical Support Directory** check box, if necessary.
  - Select the **Include Upload Failure Data Capture Directory** check box, if necessary.
5. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.

## 3 Configuring backup to a hard drive

6. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
7. Verify that the CD backup directory is correct (default directory is D:\Backup).

It is assumed that drive D is a CD-RW drive.

You can change the directory or use the **Browse** button to select another directory.

8. Install the formatted disc into the CD drive.

To back up to a writable CD, you must have CD-writing software installed. The disc must be formatted by the CD-writing software so that it behaves like a drive.

9. Click **Apply** or **OK**.

The application verifies that the backup device exists and that the server can write to it. If the device does not exist or is not writable, an error message displays that says you have entered an invalid device. Click **OK** to go back to the **Options** dialog box and fix the error.

Backup occurs, if needed, at the interval you specified.

### Configuring backup to a hard drive

---

#### NOTE

This requires a hard drive. The drive should not be the same physical drive on which your Operating System or the Management application is installed.

---

To configure the backup function to a hard drive, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.

The currently defined directory displays in the **Backup Output Directory** field.

3. Select the **Enable Backup** check box, if necessary.

4. Choose one or more of the following options:

- Select the **Include FTP Root Directory** check box.

If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.

- Select the **Include Technical Support Directory** check box, if necessary.

- Select the **Include Upload Failure Data Capture Directory** check box, if necessary.

5. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.

6. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.

7. Browse to the hard drive and directory to which you want to back up your data.
8. Click **Apply** or **OK**.

The application verifies that the backup device exists and that the server can write to it.

If the device does not exist or is not writable, an error message displays that states you have entered an invalid device. Click **OK** to go back to the Options dialog box and fix the error.

Backup occurs, if needed, at the interval you specified.

## Configuring backup to a network drive

To back up to a network drive, your workstation can be either in the same domain or in the same workgroup. However, you must have rights to copy files for the network drive.

---

### NOTE

The Management application should not directly access local or network resources through mapped drive letters. When the Management application must access a remote resource (or any process that is running in a different security context), you should use the Universal Naming Convention (UNC) name to access the resource. For more information about services and redirected drives, refer to <http://support.microsoft.com/kb/180362/en-us>.

---



---

### NOTE

Configuring backup to a network drive is not supported on UNIX systems.

---



---

### NOTE

It is recommended that this configuration be completed on the Local client (the client application running on the Server) so that the backup path and location can be confirmed.

---

To configure the backup function to a network drive, complete the following steps.

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **Backup** in the **Category** list.  
The currently defined directory displays in the **Backup Output Directory** field.
3. Select the **Enable Backup** check box, if necessary.
4. Choose one or more of the following options:
  - Select the **Include FTP Root Directory** check box.  
If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.
  - Select the **Include Technical Support Directory** check box, if necessary.
  - Select the **Include Upload Failure Data Capture Directory** check box, if necessary.
5. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.
6. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.

7. Click **Browse** to choose the network share and directory to which you want to back up your data, or enter the network share and directory path.

---

**NOTE**

You must specify the directory in a network share format (for example, \\network-name\share-name\directory). Do not use the drive letter format (C:\directory).

---

8. If you want to configure backup to a network drive on a Windows system, complete the following steps.
  - a. Enter the name of the Windows domain or workgroup in which you are defined in the **Domain Workgroup** field.

---

**NOTE**

You must be authorized to write to the network device.

---

- b. Enter your Windows login name in the **User Name** field.
  - c. Enter your Windows password in the **Password** field.
9. Click **Apply** or **OK**.

The application verifies that the device is accessible and that the server can write to it.

If the device does not exist or you are not authorized to write to the network drive, an error message displays that states you have entered an invalid device path or invalid network credentials. Click **OK** to go back to the Options dialog box and fix the error.

Backup occurs, if needed, at the interval you specified.

## Enabling backup

Backup is enabled by default. However, if it has been disabled, complete the following steps to enable the function.

1. Select **Server > Options**.

The **Options** dialog box displays.
2. Select **Backup** in the **Category** list.
3. Select the **Enable Backup** check box.
4. Click **Apply** or **OK**.

## Disabling backup





Backup is enabled by default. If you want to stop the backup process, you need to disable backup. To disable the backup function, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.
2. Select **Backup** in the **Category** list.
3. Clear the **Enable Backup** check box.
4. Click **Apply** or **OK**.

## Viewing the backup status

The Management application enables you to view the backup status at a glance by providing a backup status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the backup function.

Icon	Description
	Backup in Progress—displays the following tooltip: "Backup started at hh:mm:ss, in progress... XX directories are backed up."
	Countdown to Next Scheduled Backup—displays the following tooltip: "Next backup scheduled at hh:mm:ss."
	Backup Disabled—displays the following tooltip: "Backup is disabled."
	Backup Failed—displays the following tooltip: "Backup failed at hh:mm:ss mm/dd/yyyy."

## Changing the backup interval

When the backup feature is enabled, your SAN is protected by automatic backups. The backups occur every 24 hours by default. However, you can change the interval at which backup occurs.

### ATTENTION

Do NOT modify the backup.properties file.

To change the backup interval, complete the following steps.

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **Backup** in the **Category** list.
3. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
4. Click **Apply** or **OK**.

The minimum value is 6 hours and the maximum value is 24 hours.

### Starting immediate backup

---

**NOTE**

You must have backup privileges to use the Backup Now function.

---

To start the backup process immediately, complete one of the following procedures:

Using the Backup Icon, right-click the **Backup** icon and select **Backup Now**.

OR

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.

3. Click **Backup Now**.

The backup process begins immediately. There is no confirmation message.

4. Click **Apply** or **OK**.

### Reviewing backup events

The Master Log, which displays in the lower left area of the main window, lists the events that occur on the Fabric.

If you do not see the Master Log, select **View > All Panels**.

The following backup events appear in the Master Log:

- Backup started
- Backup error
- Backup Enabled
- Backup Disabled
- Backup Now
- Backup destination change
- Backup interval change
- Backup start time change
- Domain workgroup change
- User name change
- User password change
- Number of files backed up on completion
- Network share access problem when backup starts or during backup (not when the backup configuration is changed)

## Data restore

---

### NOTE

You cannot restore data from a previous version of the Management application.

---

### NOTE

You cannot restore data from a different edition of the Management application.

---

The Management application helps you to protect your data by backing it up automatically. The data can then be restored, as necessary.

The data in the following directories is automatically backed up to disk. The data includes the following items:

- Backup\databases — contains database and log files.
- Backup\data — contains M-EOS switches Element Manager data files (including Dump files, Data collection progress files, Director/Switch firmware files FAF files, Switch technical supportSave, and Switch backup files) and Fabric OS miscellaneous files.
- Backup\conf — contains the Management application configuration files.
- Backup\cimom — contains the SMIA configuration files.

In a disaster recovery situation, it is possible that configuration changes made less than 45 minutes before Server loss (depending on the backup interval you set) could be missing from the backup.

## Restoring data

1. (Windows) Open the **Server Management Console** from the **Start** menu on the Management application server.

OR

(UNIX) Open *Install\_Home/bin* from the Management application server and type `./smc.sh` at the command line.

2. Click the **Services** tab.

The tab lists the Management application services.

3. Click **Stop Services** to stop all of the services.

4. Click the **Restore** tab.

5. Browse to the backup location.

Browse to the location specified in the **Output Directory** field on the **Options** dialog box - Backup pane.

6. Click **Restore**.

Upon completion, a message displays the status of the restore operation. Click **OK** to close the message and the Server Management Console. For the restored data to take effect, re-launch the Configuration Wizard using the instructions in [“Launching the Configuration Wizard”](#) on page 18.

Restoring data to a new server

If your Management application server fails and you must recover information to a new server, restore the data (Refer to “Restoring data” on page 67 for complete instructions).

Display

You can configure the display for FICON and reset the display to the default settings.

Setting your FICON display

FICON display setup rearranges the columns of any table that contains end device descriptions to move the following eight columns to be the first columns: FC Address, Serial #, Tag, Device Type, Model, Vendor, Port Type, and WWN.

To set the FICON display, complete the following steps.

- 1. Select **Server > Options**.

The **Options** dialog box displays (Figure 30).

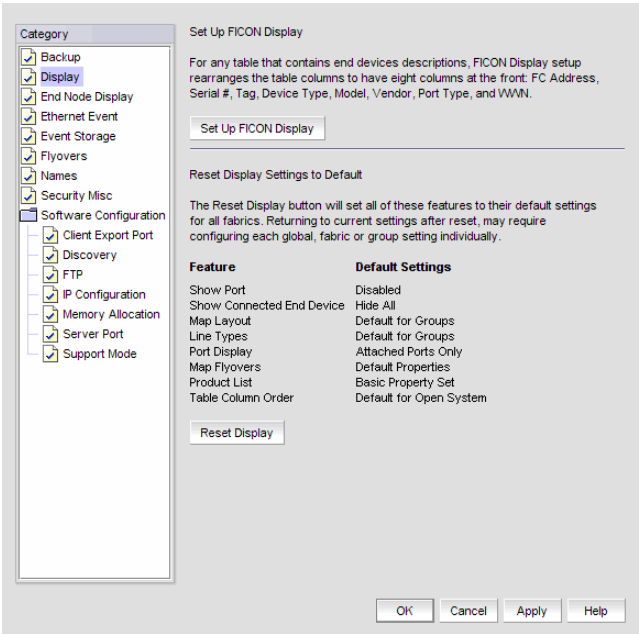


FIGURE 30 Options dialog box (Display option)

- 2. Select **Display** in the **Category** list.
- 3. Click **Set Up FICON Display**.

All tables that contain end device descriptions display the following columns as the first eight columns: FC Address, Serial #, Tag, Device Type, Model, Vendor, Port Type, and WWN.

- 4. Click **Apply** or **OK** to save your work.

## Resetting your display

You can reset your system to display the default display settings. Note that returning to current settings after a reset may require configuring each global fabric or group setting individually. The following table ([Table 7](#)) details the settings that change with reset and the associated default state.

**TABLE 7** Default Display Settings

Settings	Default State
Show port	Disabled.
Show connected end device	Set to Hide All.
Map Layout	Set to default for Groups.
Line Types	Set to default for Groups.
Port Display	Set to Attached Ports only.
Map Flyovers	Set to include the following properties: <ul style="list-style-type: none"><li>• Product Display—Name, Device Type, WWN, IP Address, and Domain ID.</li><li>• Connection Display—Name (port), Address, Node WWN, Port WWN, and Port #.</li></ul>
Product List	Set to only display basic property list.
Table Column Order	Set to default for open system.

To reset the Management application to the default display and view settings, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Display** in the **Category** list.
3. Click **Reset Display**.
4. Click **Yes** on the reset confirmation message.

The display and view settings are immediately reset to the default display settings (as detailed in the Default display Settings table ([Table 7](#))).

5. Click **Apply** or **OK** to save your work.

## End node display

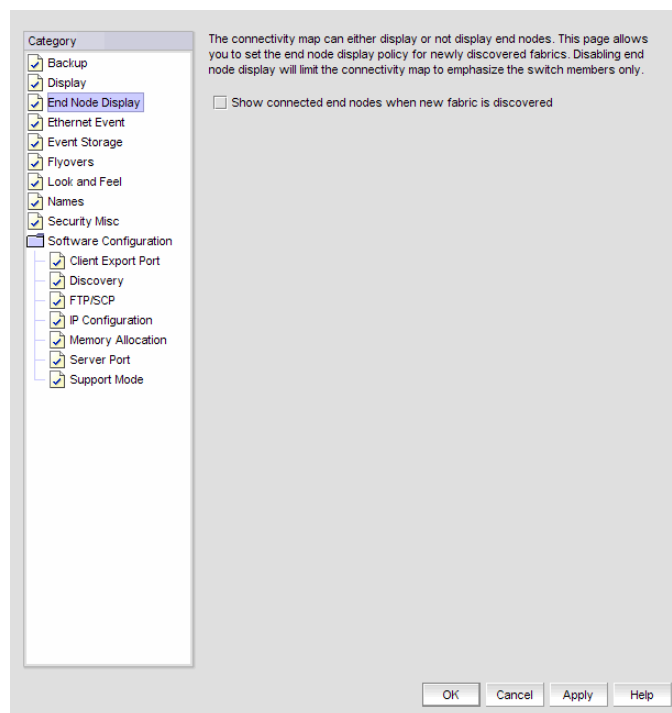
The connectivity map can be configured to display or not display end nodes. This option enables you to set the end node display for all newly discovered fabrics. Note that disabling end node display limits the connectivity map to emphasize switch members only.

### Displaying end nodes

To display end nodes when discovering a new fabric, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays (Figure 31).



**FIGURE 31** Options dialog box (End Node Display option)

2. Select **End Node Display** in the **Category** list.
3. Select the **Show connected end nodes when new fabric is discovered** check box to display end nodes on your system.

---

#### NOTE

Before changes can take effect, the topology must be rediscovered.

---

4. Click **Apply** or **OK** to save your work.

## Ethernet events

An Ethernet event occurs when the Ethernet link between the Management Server and the managed device is lost. You can configure the application to enable events when the Ethernet connection is lost.

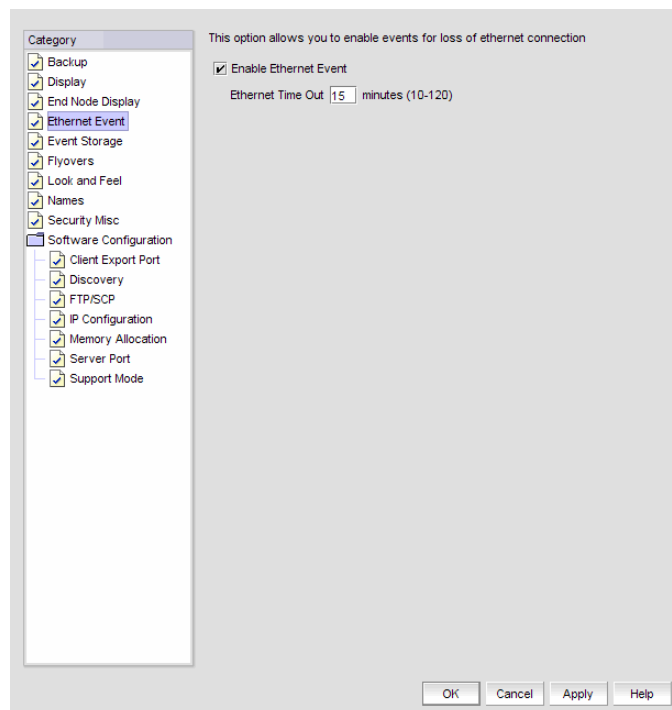
### Enabling Ethernet events

The **Options** dialog box enables you to configure the Management application to generate an Ethernet event after a device is offline for a specific period of time.

To enable Ethernet events, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays ([Figure 32](#)).



**FIGURE 32** Options dialog box (Ethernet Event option)

2. Select **Ethernet Event** in the **Category** list.
3. Select the **Enable Ethernet Event** check box.
4. Enter the Ethernet time out value (10 to 120 minutes).
5. Click **Apply** or **OK** to save your work.

## Disabling Ethernet events

To disable Ethernet events, complete the following steps.

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **Ethernet Event** in the **Category** list.
3. Clear the **Enable Ethernet Event** check box.
4. Click **Apply** or **OK** to save your work.

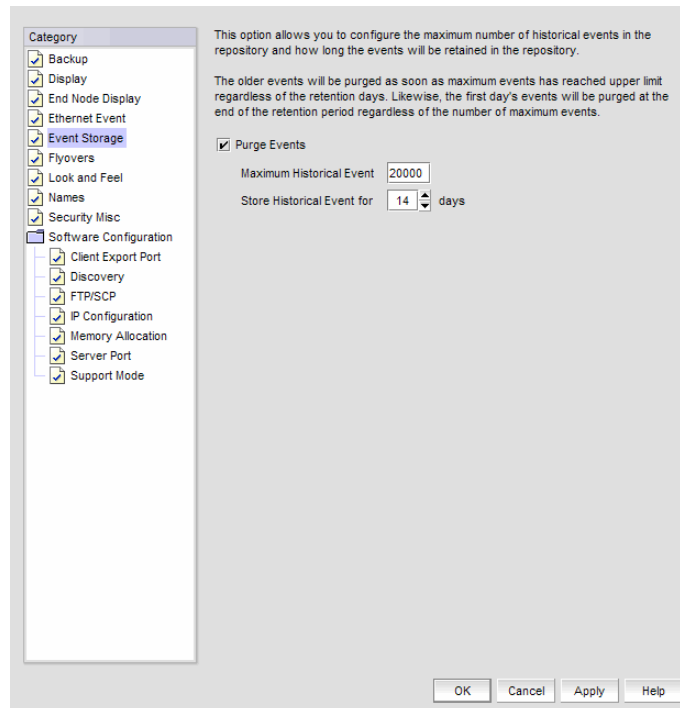
## Event storage

You can configure the number of historical events in the repository as well as how long the events will be retained.

## Configuring event storage

To configure event storage, complete the following steps.

1. Select **Server > Options**.  
The **Options** dialog box displays ([Figure 33](#)).



**FIGURE 33** Options dialog box (Event Storage option)

2. Select **Event Storage** in the **Category** list.

3. Select the **Purge Events** check box.  
Events are purged at midnight (12:00 AM). For example, when the maximum number of events allowed limit is reached at 3:00 PM, the system purges the older events at midnight that day.
4. Enter the number of events (1 through 50000) in the repository in the **Maximum Historical Event** field.  
Older events are purged at midnight on the date the maximum event limit is reached regardless of the retention days.
5. Enter then number of days (1 through 30) you want to store events in the **Store Historical Event for <number> days** field.  
The events are purged at midnight on the last day of the retention period regardless of the number of maximum events.
6. Click **OK**.

---

**NOTE**

Purged events from the event and syslog event tables are stored in the *Install\_Home\data\archive* directory. These files are retained for a maximum of 7 days.

---

## Flyovers

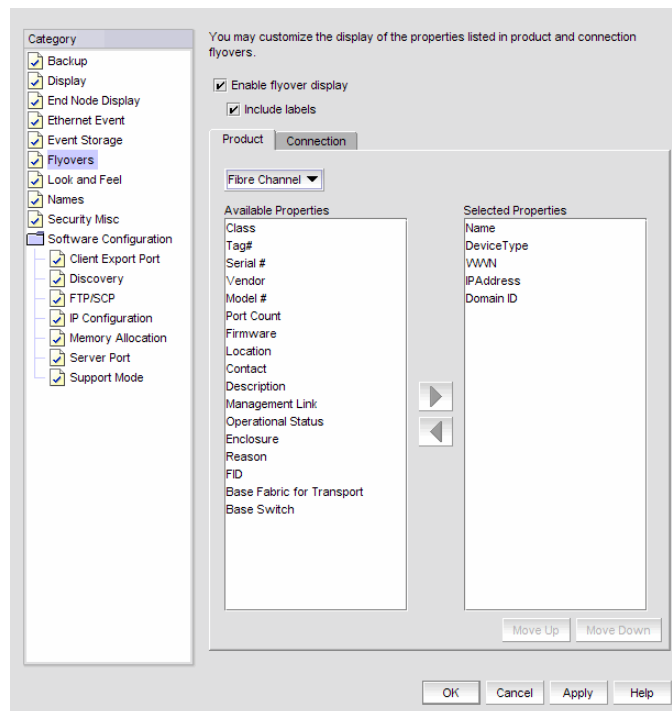
You can configure your system to display information for products and connections in a pop-up window on the Connectivity Map.

### Configuring flyovers

To display product information in a pop-up window, complete the following steps.

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **Flyovers** in the **Category** list.
3. Select the **Enable flyover display** check box to enable flyover display on your system.
4. Select the **Include labels** check box to include labels on flyover displays.

5. Select the **Product** tab (Figure 35) and complete the following steps to select the product properties you want to display on flyover.



**FIGURE 34** Options dialog box (Flyovers option, Product tab)

- a. Select each property you want to display in the product flyover from the **Available Properties** table.

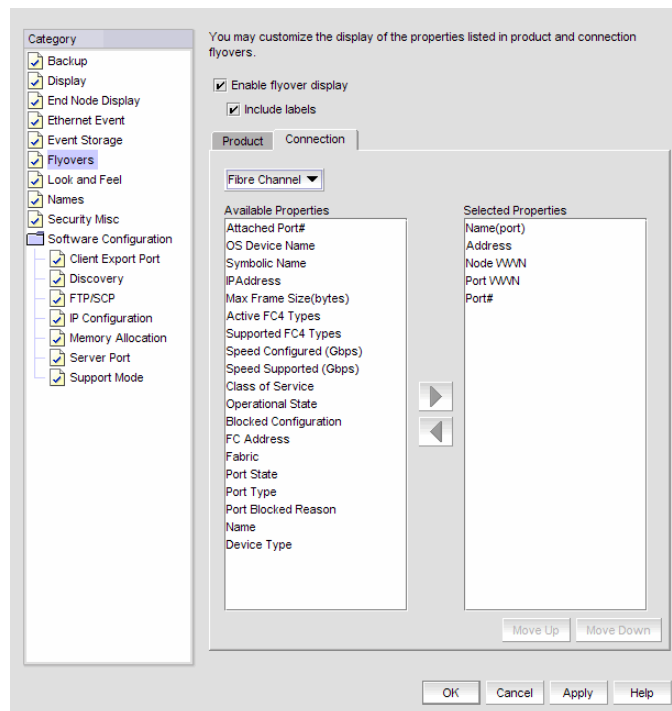
The available product properties include the following options:

- |               |                             |
|---------------|-----------------------------|
| • Name        | • Firmware                  |
| • Device Type | • Location                  |
| • WWN         | • Contact                   |
| • IP Address  | • Description               |
| • Domain ID   | • Management Link           |
| • Class       | • Operational Status        |
| • Tag#        | • Enclosure                 |
| • Serial #    | • Reason                    |
| • Vendor      | • FID                       |
| • Model #     | • Base Fabric for Transport |
| • Port Count  | • Base Switch               |
| • Seed Switch |                             |

- b. Click the right arrow to move the selected properties to the **Selected Properties** table.
- c. Use the **Move Up** and **Move Down** buttons to reorder the properties in the **Selected Properties** table, if necessary.

The properties displayed in the **Selected Properties** table appear in the flyover display.

6. Select the **Connection** tab (Figure 35) and complete the following steps to select the information you want to display on flyover.



**FIGURE 35 Options dialog box (Flyovers option, Connection tab)**

- a. Select the protocol from the **Protocol** list.

The default protocol is Fibre Channel. Depending on which protocol you select, some properties may not be available for all protocols.

- b. Select each property you want to display in the connection flyover from the **Available Properties** table.

Depending on which protocol you select, some of the following properties may not be available for all protocols:

**Fibre Channel (default)**

- |                          |                           |
|--------------------------|---------------------------|
| • Name (port)            | • Speed Configured (Gbps) |
| • Address                | • Speed Supported (Gbps)  |
| • Node WWN               | • Class of Service        |
| • Port WWN               | • Operational State       |
| • Port#                  | • Blocked Configuration   |
| • Attached Port#         | • FC Address              |
| • OS Device Name         | • Fabric                  |
| • Symbolic Name          | • Port State              |
| • IP Address             | • Port Type               |
| • Max Frame Size (bytes) | • Port Blocked Reason     |
| • Active FC4 Types       | • Name                    |
| • Supported FC4 Types    | • Device Type             |

### 3 Turning flyovers on or off

#### FCoE

- Name
- Node WWN
- MAC
- Port#
- Port Type
- FCoE Index #

- Click the right arrow to move the selected properties to the **Selected Properties** table.
- Use the **Move Up** and **Move Down** buttons to reorder the properties in the **Selected Properties** table.

The properties displayed in the **Selected Properties** table appear in the flyover display.

- Click **Apply** or **OK** to save your work.

### Turning flyovers on or off

Flyovers display when you place the cursor on a product. They provide a quick way to view a product's properties.

To turn flyovers on or off, select **Enable Flyover Display** from the **View** menu.

### Viewing flyovers

On the Connectivity Map, rest the pointer over a product icon, port, or connection.

The pop-up window containing the product, port, or connection information displays.

## Names

You can use Names as a method of providing familiar simple names to products and ports in your SAN. Using your Management application you can:

- Set names to be unique or non-unique.
- Fix duplicate names.
- Associate a name with a product or port WWN currently being discovered.
- Add a WWN and an associated name for a product or port that is not yet being discovered.
- Remove or disassociate a name from a WWN.

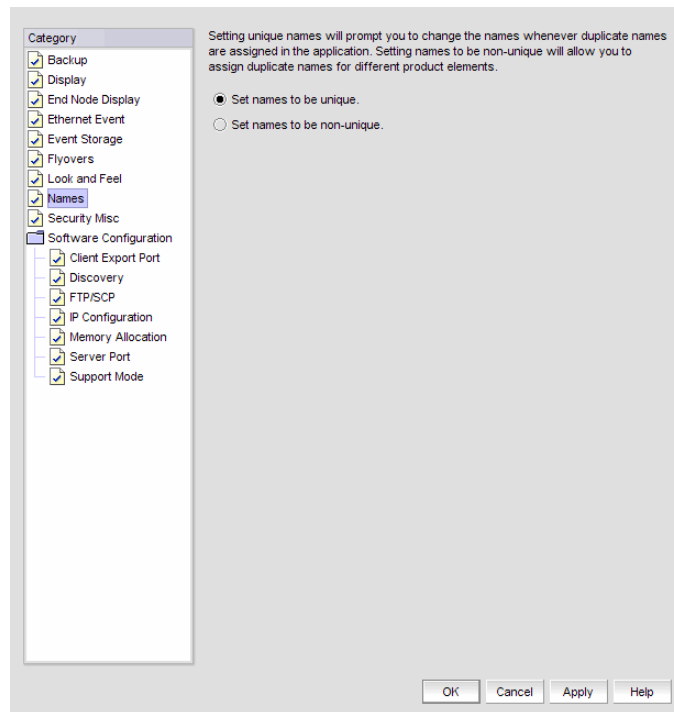
### Setting names to be unique

You can edit duplicate names so that each device has a unique name. Note that the **Duplicated Names** dialog box only displays when you set names to be unique and there are duplicate names in the system.

To edit duplicate names, complete the following steps.

- Select **Server > Options**.

The **Options** dialog box displays ([Figure 36](#)).



**FIGURE 36** Options dialog box (Names option)

2. Select **Names** in the **Category** list.
3. Select **Set names to be unique** to require that names be unique on your system.
4. Click **OK** on the **Options** dialog box.
5. Click **OK** on the “duplicate names may exist” message.  
To fix duplicated names, refer to [“Fixing duplicate names”](#) on page 78.

## Setting names to be non-unique

You can choose to allow duplicate names in your fabric.

To set names to be non-unique, complete the following steps.

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **Names** in the **Category** list.
3. Select **Set names to be non-unique** to allow duplicate names on your system.
4. Click **OK** on the **Options** dialog box.

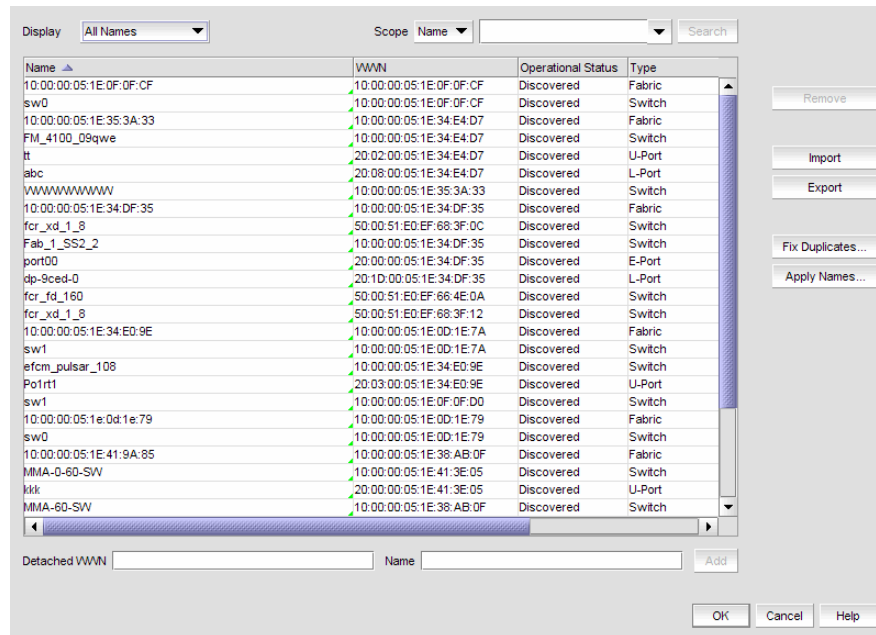
### 3 Fixing duplicate names

## Fixing duplicate names

To fix duplicated names, complete the following steps.

1. Select **Configure > Names**.

The **Configure Names** dialog box displays (Figure 37).



**FIGURE 37** Configure Names dialog box

2. Click **Fix Duplicates**.

The **Duplicated Names** dialog box displays.

3. Select one of the following options.
  - If you select **Append Incremental numbers for all repetitive names**, the names are edited automatically using incremental numbering.
  - If you select **I will fix them myself**, edit the name in the **Name** field.
4. Click **OK** on the **Duplicated Names** dialog box.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

## Viewing names

To view names associated with devices by name, complete the following steps.

1. Select **Configure > Names**.

The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.

Only devices with a name display. The table displays the Name, WWN, Operational Status, Type, and a Description of the device.

3. Click **OK** to close the **Configure Names** dialog box.

## Adding a name to an existing device

To add a name to an existing device, complete the following steps.

1. Select **Configure > Names**.

The **Configure Names** dialog box displays.

2. Select how you want to display devices from the **Display** list.

You can display devices by **All Names**, **All WWNs**, **Only Fabrics**, **Only Products**, **Only Ports**, or **Switch and N Ports**.

All discovered devices display.

3. Select the device to which you want to assign a name in the **Display** table.

4. Double-click in the **Name** column for the selected device and enter a name for the device.

If you set names to be unique on the **Options** dialog box and the name you entered already exists, the entry is not accepted. To search for the device already using the name, refer to [“Searching for a device by name”](#) on page 82 or [“Searching for a device by WWN”](#) on page 83 in the **Configure Names** dialog box or [“Searching for a device in the connectivity map”](#) on page 139 in the connectivity map.

---

### NOTE

If you segment a fabric, the Fabric's name follows the assigned principal switch.

---

5. Click **OK** on the confirmation message.
6. Click **OK** to close the **Configure Names** dialog box.

### Adding a name to a new device

To add a new device and name it, complete the following steps.

1. Select **Configure > Names**.

The **Configure Names** dialog box displays.

2. Enter the WWN of the device in the **Detached WWN** field.
3. Enter a name for the device in the **Name** field.
4. Click **Add**.

The new device displays in the table.

If you set names to be unique on the **Options** dialog box and the name you entered already exists, a message indicating the name already in use displays. Click **OK** to close the message and change the name.

5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

### Applying a name to a detached WWN

To apply a name to a detached wwn, complete the following steps.

1. Select **Configure > Names**.

The **Configure Names** dialog box displays.

2. Click **Apply Names**.

If there are any detached WWNs in a discovered state, the **Apply Names** dialog box displays.

3. Select or clear the check box for the associated switch or switch port.

Select a check box to apply the detached name as the switch or switch port name and remove the duplicated WWN entry (detached) in the **Configure Names** dialog box.

Clear a check box to remove the duplicated WWN entry (detached) in the **Configure Names** dialog box.

4. Click **OK** on the **Apply Names** dialog box.
5. Click **OK** on the **Configure Names** dialog box.

### Removing a name from a device

1. Select **Configure > Names**.

The **Configure Names** dialog box displays.

2. In the **Display** table, select the name you want to remove.
3. Click **Remove**.

An application message displays asking if you are sure you want clear the selected name.

4. Click **Yes**.

5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

## Editing names

To edit the name associated with a device, complete the following steps.

1. Select **Configure > Names**.  
The **Configure Names** dialog box displays.
2. Select **All Names** from the **Display** list.  
Only devices with a name display. The table displays the Name, WWN, Operational Status, Type, and a Description of the device.
3. Click the name you want to edit in the **Name** column.
4. Edit the name and press **Enter**.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

## Exporting names

To export the names associated with devices, complete the following steps.

1. Select **Configure > Names**.  
The **Configure Names** dialog box displays.
2. Click **Export**.  
The **Export Files** dialog displays.
3. Browse to the location where you want to save the export file.  
Depending on your operating system, the default export location are as follows:
  - Desktop\My documents (Windows)
  - \root (Linux)
  - \ (Solaris)
4. Enter a name for the file and click **Save**.
5. Click **OK** to close the **Configure Names** dialog box.

## Importing Names

If the name length exceeds the limitations detailed in the following table, you must edit the name (in the CSV file) before import. Names that exceed these limits will not be imported. If you migrated from a previous version, the .properties file is located in the *Install\_Home\migration\data* folder.

Device	Character limit
Fabric OS switch 6.2 or later	30 (24 character limit when in FICON mode)
Fabric OS switch 6.1.X or earlier	15
Fabric OS switch port	32 (24 character limit when in FICON mode)
M-EOS switch	24
M-EOS switch port	24
HBA	256
HBA port	256
Others names	128

To import names, complete the following steps.

1. Select **Configure > Names**.  
The **Configure Names** dialog box displays.
2. Click **Import**.  
The **Import Files** dialog displays.
3. Browse to the import (.csv) file location.
4. Select the file and click **Import**.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

## Searching for a device by name

You can search for objects (switch, fabric, product, ports, or N Ports) by name. To search for a name in the Connectivity Map, refer to [“Searching for a device in the connectivity map”](#) on page 139.

To search by name, complete the following steps.

1. Select **Configure > Names**.  
The **Configure Names** dialog box displays.
2. Select **All Names** from the **Display** list.
3. Select **Name** from the **Scope** list.
4. Enter the name you want to search for in the **Search** field.

You can search on partial names.

### NOTE

To search for a device, the device must be discovered and display in the topology.

5. Click **Search**.

All devices with the specified name (or partial name) are highlighted in the **Display** table. You may need to scroll to see all highlighted names.

6. Click **OK** to close the **Configure Names** dialog box.

## Searching for a device by WWN

You can search for objects (switch, fabric, product, ports, or N Ports) by WWN (world wide name). To search for a name in the Connectivity Map, refer to [“Searching for a device in the connectivity map”](#) on page 139.

To search by WWN, complete the following steps.

1. Select **Configure > Names**.

The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.
3. Select **WWN** from the **Scope** list.
4. Enter the WWN you want to search for in the **Search** field.

You can search on partial WWNs.

---

**NOTE**

To search for a device, the device must be discovered and display in the topology.

---

5. Click **Search**.

All devices with the specified WWN (or partial WWN) are highlighted in the **Display** table. You may need to scroll to see all highlighted WWNs.

6. Click **OK** to close the **Configure Names** dialog box.

# Security

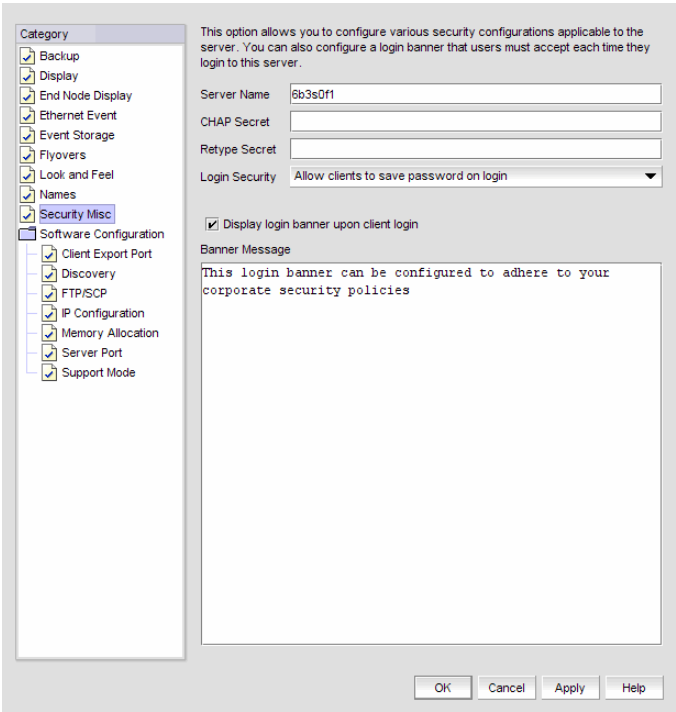
You can configure the Server Name, CHAP secret value, and login banner, and modify whether or not to allow clients to save passwords. When the login banner is enabled, each time a client connects to the server, the login banner displays with a legal notice provided by you. The client's users must acknowledge the login banner to proceed, otherwise they are logged out.

## Configuring the server name

To set the CHAP secret, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays (Figure 38).



**FIGURE 38** Options dialog box (Security Misc option)

2. Select **Security Misc** in the **Category** list.
3. Enter the server name in the **Server Name** field.

The **Server Name** field cannot be empty.

4. Enter a password in the **CHAP Secret** field.

The secret must be entered as a 32-digit hexadecimal value, or as a 16-digit ASCII value preceded by a dollar sign (\$), for example, \$abcdefghijklmnopqrstuvwxyz.

5. Re-enter the password in the **Retype Secret** field.

If the secret does not meet the application requirements or the **CHAP Secret** and **Retype Secret** entries do not match, an error message displays. Click **OK** to re-enter the **CHAP Secret** and **Retype Secret** values.

You are about to modify the ID/Secret of this server. Check all products that this server is managing and make sure the corresponding Software ID/Secret is updated appropriately. If you fail to do so, your server may not be able to manage the products any more.

6. Click **OK** on the confirmation message.
7. Click **Apply** or **OK** to save your work.

## Setting the CHAP secret

To set the CHAP secret, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Enter a password in the **CHAP Secret** field.

The secret must be entered as a 32-digit hexadecimal value, or as a 16-digit ASCII value preceded by a dollar sign (\$), for example, \$abcdefghijklmnopqrstuvwxyz.

4. Re-enter the password in the **Retype Secret** field.

If the secret does not meet the application requirements or the **CHAP Secret** and **Retype Secret** entries do not match, an error message displays. Click **OK** to re-enter the **CHAP Secret** and **Retype Secret** values.

You are about to modify the ID/Secret of this server. Check all products that this server is managing and make sure the corresponding Software ID/Secret is updated appropriately. If you fail to do so, your server may not be able to manage the products any more.

5. Click **OK** on the confirmation message.
6. Click **Apply** or **OK** to save your work.

## Configuring login security

To configure login security, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Choose one of the following options:

- To allow users to save their password in the **Login Security** list, select **Allow clients to save password on login**.
- To not allow users to save their password in the **Login Security** list, select **Do NOT allow clients to save password on login**.

4. Click **Apply** or **OK** to save your work.

### Configuring the login banner display

To configure the login banner display, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Select the **Display login banner upon client login** check box.
4. Enter the message you want to display every time a user logs into this server in the **Banner Message** field.

This field contains a maximum of 1024 characters.

5. Click **Apply** or **OK** to save your work.

### Disabling the login banner

To disable the login banner display, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Clear the **Display login banner upon client login** check box.

---

**NOTE**

Users logging into the client will not see the banner when logging in to this Server.

---

4. Click **Yes** on the confirmation message.
5. Click **Apply** or **OK** to save your work.

# Software Configuration

The Management application allows you to configure the following software settings:

- Client export port—A port for communication between the client and server.
- Discovery—HTTP or HTTP over SSL when connecting to the switch.
- FTP/SCP overview—Internal or external FTP server settings.
- IP Configuration—Configure the Ethernet ports with the IP address.
- Memory allocation—Memory allocation for the client and server.
- Server port—Server port settings.
- Support mode—Support settings to allow enhanced diagnostics.

## Client export port

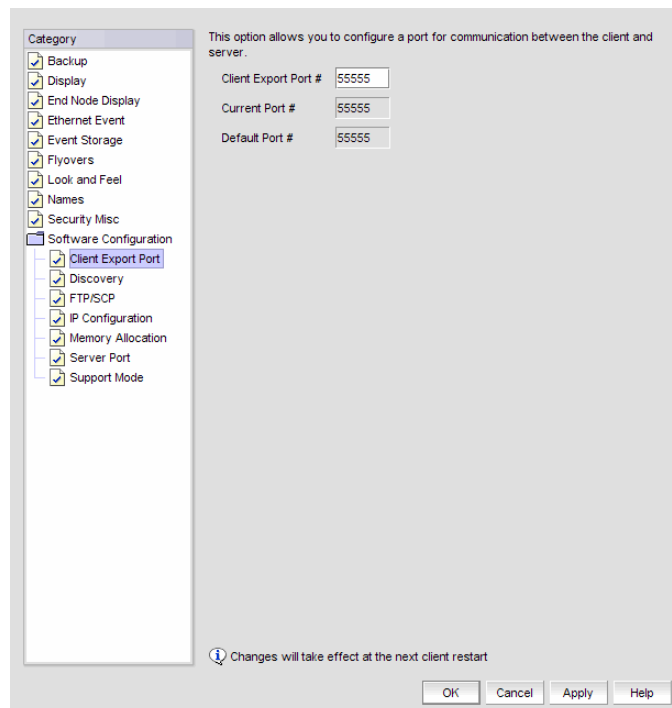
You can configure a port for communication between the client and server.

### *Configuring the client export port*

To configure client export port settings, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays ([Figure 39](#)).



**FIGURE 39** Options dialog box (Client Export Port option)

2. Select **Client Export Port** to assign a communications port between the client and server in the **Category** list.

3. Enter the client export port number to set a fixed port number for the client in the **Client Export Port** field.
4. Click **Apply** or **OK** to save your work.

## NOTE

Changes to this option take effect after a client restart.

5. Click **OK** on the “changes take effect after client restart” message.

## Discovery

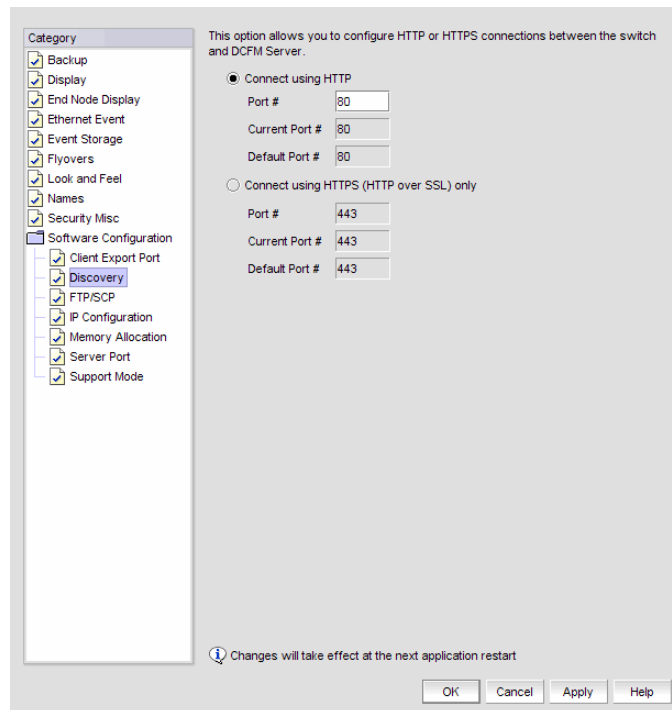
You can configure connections between the switch and the Management application server.

### Configuring Discovery

To configure discovery, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays (Figure 40).



**FIGURE 40** Options dialog box (Discovery option)

2. Select **Discovery** in the **Category** list.

3. Choose one of the following options:
  - If you want to connect using HTTP, complete the following steps.
    - a. Select the **Connect using HTTP** option.
    - a. Enter the connection port number in the **Port #** field. Continue with [step 4](#).
  - If you want to connect using HTTPS (HTTP over SSL), complete the following steps.
    - a. Select the **Connect using HTTPS (HTTP over SSL) only** option.
    - b. Enter the connection port number in the **Port #** field. Continue with [step 4](#).
4. Click **Apply** or **OK** to save your work.

---

**NOTE**

Changes to this option take effect after an application restart.

---

5. Click **OK** on the “changes take effect after application restart” message.

## FTP/SCP overview

File Transfer Protocol (FTP) is a network protocol used to transfer data from one computer to another over a TCP computer network. During installation, a built-in FTP server and its services are installed. Other FTP servers on your system are recognized by the application as external FTP servers.

For Windows systems, the built-in FTP server is the default configuration and installation starts the FTP service if port 21 is not used by any other FTP server. For UNIX systems, built-in FTP is the default for UNIX systems during installation; the external FTP server is the default only if port 21 is busy.

Note that when uninstalling the application the built-in FTP server is removed with all other services even if the FTP service is used by firmware upgrade or supportSave features.

Secure Copy (SCP) is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol. You must configure SCP on your machine to support Technical Support and firmware download.

### *Accessing the FTP server folder*

Choose from one of the following options to access the FTP server folder:

- To access the internal FTP folder, select **Monitor > Techsupport > View Repository**.
- To access the external FTP folder, type the following in a browser window:  
`ftp://Username@External_FTP_Server_IP_Address`  
 (for example, `ftp://admin@10.1.1.1`) and press **Enter**. Type your password in the pop-up window and press **Enter**. The external FTP folder displays.

## Configuring an internal FTP server

To configure the internal FTP server settings, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays (Figure 41).

**FIGURE 41** Options dialog box (FTP/SCP option)

2. Select **FTP/SCP** in the **Category** list.
3. Select the **Use built-in FTP Server** option to use the default built-in FTP server.  
All active fields are mandatory.
4. Change your password by entering a new password in the **Password** and **Confirm Password** fields.
5. Click **Test** to test the FTP server.  
An “FTP Server running successfully” or an error message displays.  
If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.
6. Click **Apply** or **OK** to save your work.

### *Configuring an external FTP server*

To configure the external FTP server settings, complete the following steps.

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **FTP/SCP** in the **Category** list.
3. Select the **Use External FTP Server and/or SCP Server** option.
4. Select the **External FTP Server** check box to configure the external FTP server.  
All fields are mandatory.
5. Enter the IP address for the remote host in the **Remote Host IP** field.
6. Enter a user name in the **Remote User Name** field.
7. Enter the path to the remote host in the **Remote Directory Path** field.  
Use a slash (/) or a period ( . ) to denote the relative root directory of the FTP server. Do not give an absolute path.
8. Enter the password in the **Password Required for FTP** field.
9. Click **Test** to test the FTP server.  
An "FTP Server running successfully" or an error message displays.  
If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.
10. Click **OK** on the message.
11. Click **Apply** or **OK** to save your work.

### *Configuring a FTP or SCP server*

To configure the SCP server settings, complete the following steps.

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **FTP/SCP** in the **Category** list.
3. Select the **Use External FTP Server and/or SCP Server** option.
4. Select the **FTP Server** check box to configure the external FTP server.  
All fields are mandatory.
5. Enter the IP address for the remote host in the **Remote Host IP** field.
6. Enter a user name in the **Remote User Name** field.
7. Enter the path to the remote host in the **Remote Directory Path** field.  
Use a slash (/) or period ( . ) to denote the root directory. Do not give an absolute path.
8. Enter the password in the **Password Required for FTP** field.

9. Click **Test** to test the FTP server.

A “Server running successfully” or an error message displays.

If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

10. Click **OK** on the message.
11. Click **Apply** or **OK** to save your work.

### *Testing the FTP and SCP server*

To test the FTP and SCP server, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **FTP/SCP** in the **Category** list.
3. Choose one or more of the following options:

- If you are using the internal FTP server, select the **Use built-in FTP Server** option.

For step-by-step instructions about configuring the built-in server, refer to [“Configuring an internal FTP server”](#) on page 90.

- If you are using the external FTP server, select the **Use External FTP Server** option.

For step-by-step instructions about configuring the built-in server, refer to [“Configuring an external FTP server”](#) on page 91.

4. Click **Test**.

An “FTP or SCP Server running successfully” or an error message displays.

If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

5. Click **OK** on the message.
6. Click **OK** to close the **Options** dialog.

## IP Configuration

You can configure IP Configuration settings.

### *Configuring IP Configuration settings*

#### NOTE

The server binds using IPv6 address by default if your Operating System is IPv6-enabled (dual mode or IPv6 only). The server binds using IPv4 address by default if your Operating System is IPv4-enabled. Servers running in dual mode allow the client to communicate from both IPv6 and IPv4 addresses.

To configure the IP address used by the server for client-server communications, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays (Figure 42).

This option allows you to configure IP Configuration settings.

Category

- ☒ Backup
- ☒ Display
- ☒ End Node Display
- ☒ Ethernet Event
- ☒ Event Storage
- ☒ Flyovers
- ☒ Look and Feel
- ☒ Names
- ☒ Security Misc
- ☒ Software Configuration
  - ☒ Client Export Port
  - ☒ Discovery
  - ☒ FTP/SCP
  - ☒ IP Configuration
  - ☒ Memory Allocation
  - ☒ Server Port
  - ☒ Support Mode

Server IP Configuration: All

Default: All

Server IP: 172.16.114.145

Server Name: 6b3s0f1

Client - Server IP Configuration

Return Address: 6b3s0f1

Current Return Address: 6b3s0f1

Switch - Server IP Configuration

Preferred Address: 172.16.114.145

If DNS is not configured in your network, do not choose the Return Address as hostname and the DCFM Server IP must bind with the host IP Address and not the hostname.

Except "Preferred Address", all other changes will take effect at the next application restart.

OK Cancel Apply Help

**FIGURE 42** Options dialog box (IP Configuration option)

2. Select **IP Configuration** in the **Category** list to set the IP address.

3. Choose one of the following options in the **Server IP Configuration** list.

- Select **All**. Go to [step 4](#).
- Select a specific IP address. Continue with [step 5](#).
- Select **localhost**. Continue with [step 5](#).

When **Server IP Configuration** is set to **All**, you can select any available IP address as the **Return Address**. If you select a specific IP address, the **Return Address** list shows the same IP address and you cannot change it.

4. Select the return IP address in the **Client - Server IP Configuration Return Address** list.
5. Select the preferred IP address in the **Switch - Server IP Configuration Preferred Address** list.

If DNS is not configured for your network, do not select the 'hostname' option from either the **Return Address** or **Preferred Address** list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.

6. Click **Apply** or **OK** to save your work.

---

**NOTE**

Changes to this option take effect after an application restart.

---

7. Click **OK** on the "changes take effect after application restart" message.

### *Configuring an explicit server IP address*

If you selected a specific IP address from the **Server IP Configuration** screen during installation and the selected IP address changes, you will not be able to connect to the server. To connect to the new IP address, you must manually update the IP address information.

To change the IP address, complete the following steps.

1. Choose one of the following options:
  - On Windows systems, select **Start > Programs > Management\_Application 10.X.X > Management\_Application Configuration**.
  - On UNIX systems, execute `sh Install_Home/bin/configwizard` in terminal.
2. Click **Next** on the **Welcome** screen.
3. Click **Yes** on the confirmation message.
4. Click **Next** on the **FTP Server** screen.
5. Complete the following steps on the **Server IP Configuration** screen ([Figure 43](#)).

**FIGURE 43** Server IP Configuration screen

- a. Select an address from the **Server IP Configuration** list.
- b. Select an address from the **Switch - Server IP Configuration Preferred Address** list.

If DNS is not configured for your network, do not select the “hostname” option from either the **Server IP Configuration** or **Switch - Server IP Configuration Preferred Address** list. Selecting the “hostname” option prevents clients and devices from communicating with the server.

- c. Click **Next**.
6. Click **Next** on the **Server Configuration** screen.
7. Click **Next** on the **SMI Agent Configuration** screen.
8. Verify your configuration information on the **Server Configuration Summary** screen and click **Next**.
9. Click **Finish** on the **Start Server** screen.
10. Click **Yes** on the restart server confirmation message.
11. Enter your user name and password.  
The defaults are **Administrator** and **password**, respectively.
12. Click **Login**.
13. Click **OK** on the Login Banner.

### *Configuring the application to use dual network cards*

Issues with Client-to-Server connectivity can be due to different reasons. Some examples are:

- The computer running the Server has more than one network interface card (NIC) installed.
- The computer running the Server is behind a firewall that performs network address translation.

To make sure that Clients can connect to the Server, you may need to edit the IP configuration setting in the **Options** dialog to manually specify the IP address that the Server should use to communicate to its Clients.

---

#### **NOTE**

The server binds using IPv6 address by default if your Operating System is IPv6-enabled (dual mode or IPv6 only). The server binds using IPv4 address by default if your Operating System is IPv4-enabled. Servers running in dual mode allow the client to communicate from both IPv6 and IPv4 addresses.

---

To configure the IP address to override the default RMI server host IP address, complete the following steps.

---

#### **NOTE**

This configuration option replaces the `-Djava.rmi.server.hostname` value used in previous releases.

---

1. Select **Server > Options**.  
The **Options** dialog box displays.
2. Select **IP Configuration** in the **Category** list to set the IP address.
3. Choose one of the following options in the **Server IP Configuration** list.
  - Select **All**. Go to [step 4](#).
  - Select a specific IP address. Continue with [step 5](#).
  - Select **localhost**. Continue with [step 5](#).

When **Server IP Configuration** is set to **All**, you can select any available IP address as the **Return Address**. If you select a specific IP address, the **Return Address** field shows the same IP address and you cannot change it.

4. Select the return IP address in the **Client - Server IP Configuration Return Address** list.
5. Click **Apply** or **OK** to save your work.

---

#### **NOTE**

Changes take effect after you restart the Management Server.

---

6. Click **OK** on the “changes take effect after “application restart” message.

## Memory allocation

You can configure memory allocation for the client and server to improve performance. You can trigger switch polling when a state changes or you can poll at intervals when no state change occurs.

### NOTE

SAN size is a consideration in selection of polling periods.

### *Configuring memory allocation settings*

To configure memory allocation settings, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays (Figure 44).

2. Select **Memory Allocation** in the **Category** list to set the memory allocation for the server and client.

This option allows you to configure memory allocation for the client and server to improve application performance. You can trigger switch polling when a state changes or you can poll at intervals when no state change occurs. SAN size is a consideration in selecting polling periods.

Current SAN Size is	Medium ▼
Client Memory Allocation	512 MB
Current Value	512
Default Minimum	512
Server Memory Allocation	768 MB
Current Value	768
Default Minimum	768
Server IP	172.16.114.46
Server Name	6b3e0f1
<b>Asset Polling</b>	
Check for state change every	120 seconds
If no state change, Poll switch every	900 seconds

Changes will take effect at the next application restart

OK Cancel Apply Help

**FIGURE 44** Options dialog box (Memory Allocation option)

3. Select the size of the SAN (small, medium, or large) you want to configure in the **Current SAN Size is** list.

Memory and asset polling values change to the new default values when you change the SAN size. You may increase these values.

4. Click **OK** on the confirmation message.

### 3 Memory allocation

5. Enter the memory allocation (MB) for the client in the **Client Memory Allocation** field.

If you enter an invalid value, an error message displays with the minimum value allowed. Click **OK** and edit the value again.

Minimum values are as follows:

- Small: 512 MB
- Medium: 512 MB
- Large: 768 MB

6. Enter the memory allocation (MB) for the server in the **Server Memory Allocation** field.

If your server has a minimum of 2 Gb RAM, change the default server memory value to 1024 MB. If your server is running less than 2 Gb RAM, do not change the default (512 MB).

Do not exceed the following server memory values:

- For Windows systems, the maximum server memory allocation is 1.4 GB.
- For UNIX systems, the maximum server memory allocation is 2 GB.

If you enter an invalid value, an error message displays with the minimum value allowed. Click **OK** and edit the value again.

Minimum values are as follows:

- Small: 768 MB
- Medium: 768 MB
- Large: 1024 MB

7. Click **Apply** or **OK** to save your work.

---

**NOTE**

Changes to this option take effect after an application restart.

---

8. Click **OK** on the “changes take effect after application restart” message.

### *Configuring asset polling*

Asset polling allows you set the length of time between state change polling. To maximize the efficiency of the polling feature (balance the amount of possible information with any possible performance impact), base your settings on the size of the SAN.

To configure asset polling, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays.

2. Select **Memory Allocation** in the **Category** list to set the memory allocation for the server and client.
3. Enter how often you want to check for state changes in the **Check for state change every** field.

You cannot enter a value lower than the default minimum value.

Default minimum values are as follows:

- Small: 60 seconds
- Medium: 120 seconds
- Large: 180 seconds

4. Enter how often you want to check for state changes in the **If no state change, Poll switch every** field.

Default values are as follows:

- Small: 120 seconds
- Medium: 900 seconds
- Large: 1800 seconds

5. Click **Apply** or **OK** to save your work.

---

**NOTE**

Changes to this option take effect after an application restart.

---

6. Click **OK** on the “changes take effect after application restart” message.

## Server port

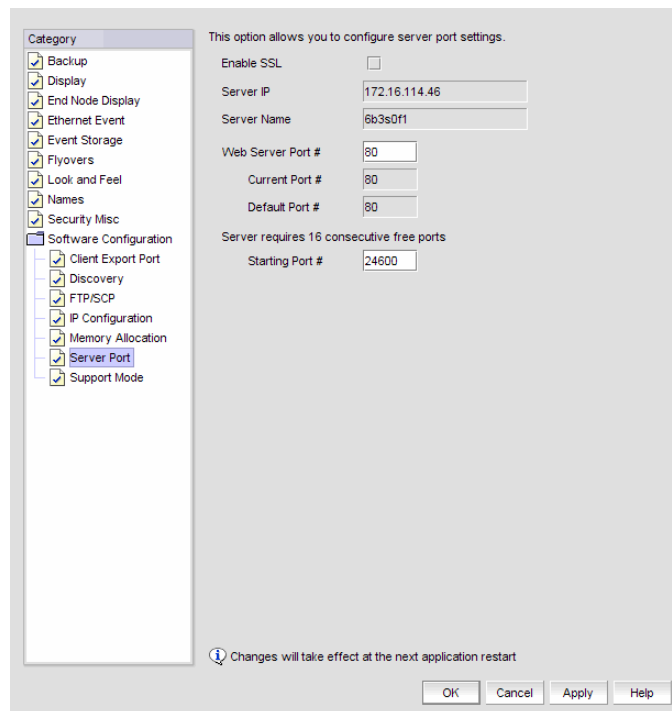
You can configure the server port settings so that you can assign a web server port number and set the server port to be SSL-enabled.

### *Configuring the server port*

To configure server settings, complete the following steps.

1. Select **Server > Options**.

The **Options** dialog box displays (Figure 45).



**FIGURE 45** Options dialog box (Server Port option)

2. Select **Server Port** in the **Category** list.
3. Select the **Enable SSL** check box to enable this function for the server port.
4. Enter a port number in the **Web Server Port #** field.

#### **NOTE**

Do not use port 2638 for any of these port numbers. Port 2638 is used internally by the server.

5. Enter a port number in the **Starting Port #** field.

The server requires 13 consecutive free ports beginning with the starting port number.

- Click **Apply** or **OK** to save your work.

---

**NOTE**

Changes to this option take effect after application restart.

---

- Click **OK** on the “changes take effect after application restart” message.

## Support mode

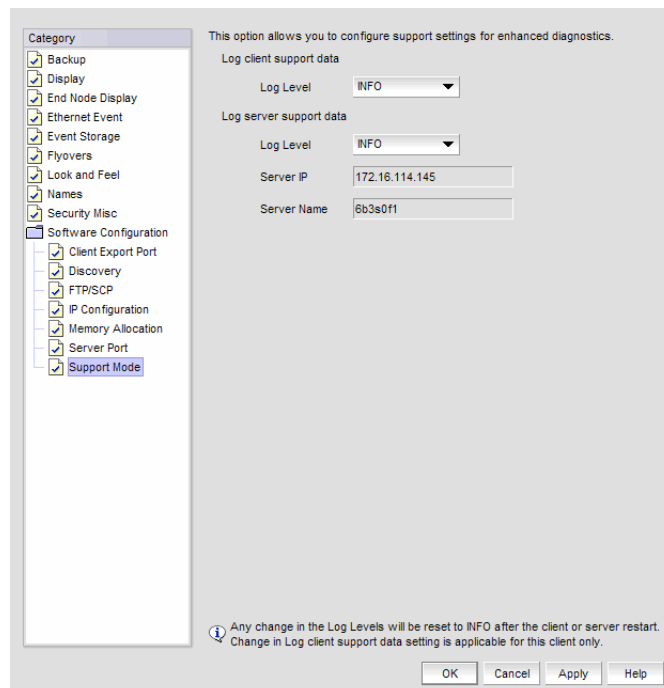
You can configure support settings to allow enhanced diagnostics.

### *Configuring support mode settings*

To configure support mode settings, complete the following steps.

- Select **Server > Options**.

The **Options** dialog box displays (Figure 46).



**FIGURE 46** Options dialog box (Support Mode option)

- Select **Support Mode** in the **Category** list to enable or disable support modes.

---

**NOTE**

Only use this option when directed to by customer support.

---

- 3. Select the **Log client support data - Log Level** list, and select the type of log data you want to configure.  
  
Log level options include: **All, Fatal, Error, Warn, Info, Debug, Trace, and Off.** Default is **Info.**  
  
The log level options return to the default value (Info) when the client or server is restarted.
- 4. Select the **Log server support data - Log Level** list, and select the type of log data you want to configure.  
  
Log level options include: **All, Fatal, Error, Warn, Info, Debug, Trace, and Off.** Default is **Info.**
- 5. Click **Apply** or **OK** to save your work.

---

**NOTE**  
Changes to the **Log client support data** or **Log server support data** log levels reset to the default (INFO) after a client or server restart.

---

---

**NOTE**  
Changes to the **Log client support data** log level is applicable for this client only.

---

Each log file (except the server log file) is limited to 5 MB. The server log file is limited to 10 MB. When a file reaches the maximum size, and there are less than 10 files for the server or 5 files for the client, a new file is created.



For web clients, log files (client.log.1 through client.log.5) are created in the *Install\_Home\Server\_Name* directory.

For clients, log files (client.log.1 through client.log.5) are created in the *User\_Home* directory.

For servers, log files (server.log.1 through server.log.10) are created in the *User\_home\jboss\server\dcn\log* directory.

## Fabric tracking

When you discover a new fabric and initial discovery is complete, fabric tracking is automatically enabled. Subsequently, if a switch or end-device is added to or removed from the fabric, a plus (+) or minus (-) icon displays (see table below) next to the product icon. Connections are also tracked. A new connection displays a solid gray line with a added icon and missing connections display a yellow dashed line with a removed icon.

	Device Added
	Device Removed

When you enable fabric tracking and a switch is missing from the fabric, a warning level call home event (Switch Switch\_WWN is missing from the fabric Fabric\_Name) is generated in the Master Log and a call home alert is sent to the corresponding call center for this event.

To avoid call home events for missing switches, create a call home event filter and clear the 'Switch is missing from the Fabric' check box in the Available Call Home Event Types table. Once you create the call home event filter, assign it to the appropriate call center. To create a call home event filter, refer to [“Defining an event filter”](#) on page 119.

## Enabling fabric tracking

1. Enable fabric tracking by choosing one of the following options:
  - Select a fabric on the Product List or Connectivity Map and select **Monitor > Track Fabric Changes**.
  - Right-click a fabric on the Product List or Connectivity Map and select **Track Fabric Changes**.

The **Accept Changes Summary** dialog box displays. This dialog box includes the following information:

- **Fabric Name**—Displays the name of the selected fabric.
  - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (+) or removed (−) from the fabric), name, IP address, WWN, and domain ID.
  - **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (+) or removed (−) from the fabric), device type, port, port WWN, node WWN, and attached port number.
  - **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (+) or removed (−) from the fabric) and connection type as well as the WWN, domain ID, IP address, and port number of the connected switches.
2. Click **Yes** to accept changes.

## Disabling fabric tracking

1. Disable fabric tracking by choosing one of the following options:
  - Select the fabric on which you want to disable fabric tracking on the Product List or Connectivity Map and select **Monitor > Track Fabric Changes**.
  - Right-click the fabric on which you want to disable fabric tracking on the Product List or Connectivity Map and select **Track Fabric Changes**.

The **Accept Changes Summary** dialog box displays. This dialog box includes the following information:

- **Fabric Name**—Displays the name of the selected fabric.
  - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (+) or removed (−) from the fabric), name, IP address, WWN, and domain ID.
  - **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (+) or removed (−) from the fabric), device type, port, port WWN, node WWN, and attached port number.
  - **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (+) or removed (−) from the fabric) and connection type as well as the WWN, domain ID, IP address, and port number of the connected switches.
2. Click **Yes**.

## Accepting changes for a fabric

1. Accept the changes to a fabric by choosing one of the following options:
  - Select a fabric on the Product List or Connectivity Map and select **Monitor > Accept Changes**.
  - Right-click a fabric on the Product List or Connectivity Map and select **Accept Changes**.

The **Accept Changes Summary** dialog box displays. This dialog box includes the following information:

- **Fabric Name**—Displays the name of the selected fabric.
  - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (+) or removed (-) from the fabric), name, IP address, WWN, and domain ID.
  - **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (+) or removed (-) from the fabric), device type, port, port WWN, node WWN, and attached port number.
  - **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (+) or removed (-) from the fabric) and connection type as well as the WWN, domain ID, IP address, and port number of the connected switches.
2. Click **Yes** to accept changes.

## Accepting changes for a device

1. Accept the changes to a device by choosing one of the following options:
  - Select the device on the Product List or Connectivity Map and select **Monitor > Accept Changes**.
  - Right-click the device on the Product List or Connectivity Map and select **Accept Change**.

The **Accept Changes Summary** dialog box displays. This dialog box includes the following information:

- **Fabric Name**—Displays the name of the selected fabric.
  - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (+) or removed (-) from the fabric), name, IP address, WWN, and domain ID.
  - **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (+) or removed (-) from the fabric), device type, port, port WWN, node WWN, and attached port number.
  - **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (+) or removed (-) from the fabric) and connection type as well as the WWN, domain ID, IP address, and port number of the connected switches.
2. Click **Yes** to accept changes.

# Call Home

---

## In this chapter

• About call home . . . . .	106
• Showing a call home center . . . . .	108
• Hiding a call home center . . . . .	109
• Editing a call home center . . . . .	109
• Enabling a call home center . . . . .	115
• Enabling support save . . . . .	115
• Testing the call home center connection . . . . .	116
• Disabling a call home center . . . . .	116
• Viewing Call Home status . . . . .	117
• Assigning a device to the call home center . . . . .	118
• Removing a device from a call home center . . . . .	118
• Removing all devices and filters from a call home center . . . . .	119
• Defining an event filter . . . . .	119
• Assigning an event filter to a call home center . . . . .	120
• Assigning an event filter to a device . . . . .	120
• Overwriting an assigned event filter . . . . .	121
• Removing an event filter from a call home center . . . . .	121
• Removing an event filter from a device . . . . .	122
• Removing an event filter from the Call Home Event Filters table . . . . .	122
• Searching for an assigned Event Filter . . . . .	122

## About call home

---

**NOTE**

Call Home is supported on Windows systems for all modem and E-mail call home centers and is supported on Linux and Solaris for the E-mail call home centers.

---

Call Home notification allows you to configure the Management application Server to automatically send an e-mail or dial-in to a support center to report system problems on specified devices (switches, routers, and directors). If you are upgrading from a previous release, all of your Call Home settings are preserved.

Call Home supports multiple call home centers which allows you to configure different devices to contact different call home centers. When you make any call home configuration changes or a call home event trigger occurs, the Management application generates an entry to the Master Log.

You can configure Call Home for the following call home centers:

- Brocade E-mail (Windows, Linux, and Solaris)
- Brocade International (Windows only)
- Brocade North America (Windows only)
- EMC (Windows only)
- HP LAN (Windows only)
- IBM (Windows only)
- IBM E-mail (Windows, Linux, and Solaris)
- SUN E-mail (Windows, Linux, and Solaris)

When configuring modem and LAN Call Home centers, you must enter the customer contact information in the device's Element Manager. You may also need to configure the Management application server IP address manually as a SNMP trap recipient for Fabric OS devices.

Call Home, using the Event Management feature, allows you to automate tasks that occur when the call home event trigger is fired. When a call home event trigger occurs, the Management application generates the following actions:

- Sends an e-mail to a specified recipient or dials-in to a support center.
- Triggers supportSave on the switch (if supportSave is enabled on the switch) prior to sending an alert. The supportSave location is included in the alert.

---

**NOTE**

The HP LAN Call Home alert displays the directory separation characters with a double backslash (\\) instead of a single backslash (\).

---

- Launches the specified application using a script.

---

**NOTE**

Launch scripts with a user interface are not supported.

---

- Adds an entry to the Master Log file and screen display.
- Generates a XML report (only available with EMC call centers) with the switch details which is sent with the E-mail.
- Generates an HTML report for E-mail-based Call Home centers.

For more information about Call Home events, refer to [“Call Home Event Tables”](#) on page 695. For more information about Event Management, refer to [“Fault Management”](#) on page 247.

Call Home allows you to perform the following tasks:

- Assign devices to and remove devices from the call home centers.
- Define filters from the list of events generated by Fabric OS and M-EOS devices.
- Edit and remove filters available in the Call Home Event Filters table.
- Apply filters to and remove filters from the devices individually or in groups.
- Edit individual call home center parameters to dial a specified phone number or E-mail a specific recipient.
- Enable and disable individual devices from contacting the assigned call home centers.
- Show or hide call home centers on the display.
- Enable and disable call home centers.

## System requirements

Call Home (except for E-Mail and HP LAN) requires the following hardware equipment:

- Any Windows Server with an internal / external modem connection
- Analog phone line

# Showing a call home center

To show a call home center, complete the following steps.

- 1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays (Figure 47).

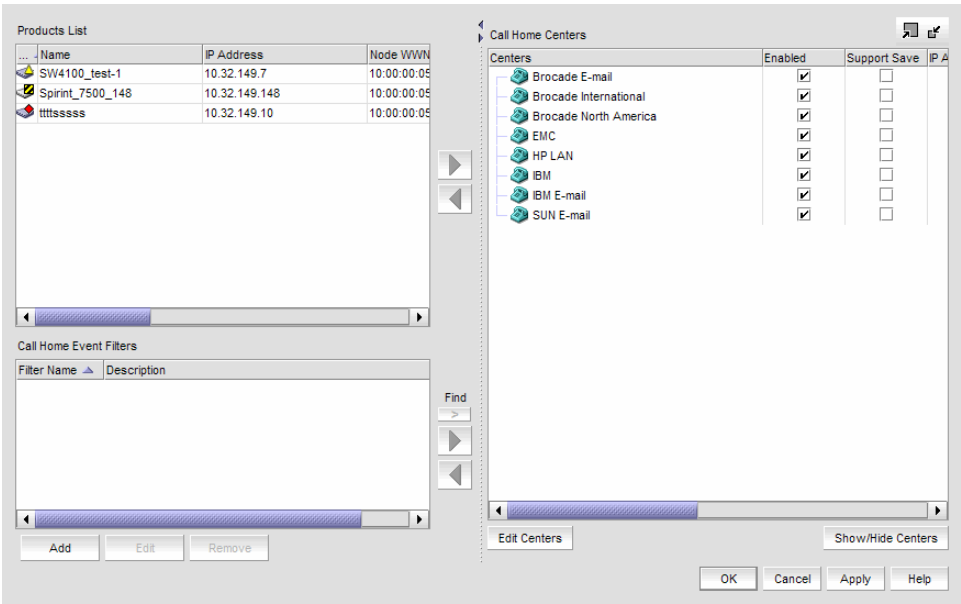


FIGURE 47 Call Home dialog box

- 2. Click **Show/Hide Centers** (beneath the **Call Home Centers** table).

The **Centers** dialog box displays with a predefined list of call home centers (Figure 48).

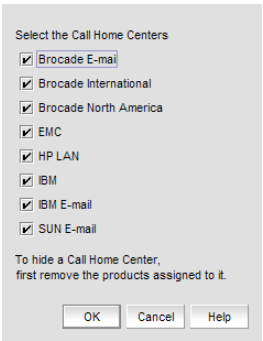


FIGURE 48 Centers dialog box

- 3. Select the check boxes of the call home centers you want to display and click **OK**.

The **Call Home** dialog box displays with the selected call home center listed in the **Call Home Centers** table.

# Hiding a call home center

**NOTE**  
Before you can hide a call home center, you must remove all assigned products.

To hide a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Click **Show/Hide Centers** (beneath the **Call Home Centers** table).  
The **Centers** dialog box displays with a predefined list of call home centers.
3. Clear the check boxes of the call home centers you want to hide and click **OK**.  
The **Call Home** dialog box displays with only selected call home centers listed in the **Call Home Centers** table.

# Editing a call home center

**NOTE**  
Call Home is supported on Windows systems for all modem call home centers and is supported on Linux and Solaris for the E-mail call home centers.

To edit a call home center, select from the following procedures:

- Editing the Brocade International or IBM call home center .....109
- Editing the Brocade North America call home center.....111
- Editing an E-mail call home center.....112
- Editing the EMC call home center .....113
- Editing the HP LAN call home center .....114

## Editing the Brocade International or IBM call home center

To edit a Brocade International or IBM call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Select the call home center you want to edit (**Brocade International** or **IBM**) in the **Call Home Centers** table.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).  
The **Configure Call Home Center** dialog box displays ([Figure 49](#)).

## 4 Editing the Brocade International or IBM call home center

Call Home Centers: Brocade International [v] Enable [x]

☐ Set heartbeat interval at 1 days (1-28)

Time Out: 60 Sec

Retry Interval: 10 Sec

Maximum Retries: 3

Call Home Center

Primary Connection: [ ]

Backup Connection: [ ]

Send Test

Local Server

Phone Number: [ ]

Server ID: 0099998

OK Cancel Apply Help

**FIGURE 49** Configure Call Home Center dialog box (Brocade International or IBM option)

4. Make sure the call home center type you selected displays in the **Call Home Centers** list.
5. Select **Enable** to enable this call home center.
6. Set the time interval at which to check the call home center by selecting the **Set the heartbeat interval at \_\_\_ days (1-28)** check box and entering the interval in the field.
7. Enter the time out interval (default is 60 seconds) in the **Time Out** field.
8. Enter the retry interval (default is 10 seconds) in the **Retry Interval** field.
9. Enter the maximum number of retries (default is 3) in the **Maximum Retries** field.
10. Enter the primary phone number or extension of the call home center in the **Call Home Center - Primary Connection** field.
11. Enter the backup phone number or extension of the call home center in the **Call Home Center - Backup Connection** field.
12. Enter the phone number or extension of the local server in the **Local Server - Phone Number** field.
13. Enter the identification number of the local server in the **Local Server - Server ID** field.
14. Click **Send Test** to test the phone number.

The selected call home center must be enabled to test the phone number.

A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

15. Click **OK**.

The **Call Home** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

16. Click **OK** to close the **Call Home** dialog box.

## Editing the Brocade North America call home center

Modem call home centers are only available for Brocade. To edit this call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select **Brocade North America** in the **Call Home Centers** table.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).

The **Configure Call Home Center** dialog box displays (Figure 50).

**FIGURE 50** Configure Call Home Center dialog box (Brocade North America option)

4. Make sure the call home center type you selected displays in the **Call Home Centers** list.
5. Select **Enable** to enable this call home center.
6. Enter the phone number or extension of the call home center in the **Call Home Center - Phone Number** field.
7. Enter the phone number or extension of the local server in the **Local Server - Phone Number** field.
8. Click **Send Test** to test the phone number.

The selected call home center must be enabled to test the phone number.

A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

9. Click **OK**.

The **Call Home** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

10. Click **OK** to close the **Call Home** dialog box.

## Editing an E-mail call home center

E-mail call home centers are available for Brocade, IBM, and SUN. To edit one of these call home centers, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select the call home center you want to edit (**Brocade E-mail**, **IBM E-mail**, or **SUN E-mail**) in the **Call Home Centers** table.

3. Click **Edit Centers** (beneath the **Call Home Centers** table).

The **Configure Call Home Center** dialog box displays ([Figure 51](#)).

**FIGURE 51** Configure Call Home Center dialog box (Brocade, IBM, or SUN E-mail option)

4. Make sure the call home center type you selected displays in the **Call Home Centers** list.
5. Select the **Enable** check box to enable this call home center.
6. Enter the customer contact name in the **Customer Details - Name** field.
7. Enter the company name in the **Customer Details - Company** field.
8. Enter the phone number of the customer contact in the **Customer Details - Phone (Office)** field.
9. Enter the mobile phone number of the customer contact in the **Customer Details - Phone (Mobile)** field.
10. Enter the name of the server in the **SMTP Server Settings - Server Name** field.
11. Select the **SMTP over SSL** check box to enable secure communication between the SMTP server and the Management application.
12. Enter the port number (default is 465 if SMTP over SSL is enabled; otherwise, the default is 25) of the server in the **SMTP Server Settings - Port** field.
13. Enter a user name in the **SMTP Server Settings - Username** field.

This is a required field when the SMTP server authentication is enabled.

14. Enter a password in the **SMTP Server Settings - Password** field.

This is a required field when the SMTP server authentication is enabled.

15. Enter the e-mail address for replies in the **E-mail Notification Settings - Reply Address** field.
16. Enter the customer e-mail address in the **E-mail Notification Settings - Send To Address** field.
17. Click **Send Test** to test the mail server.

The selected call home center must be enabled to test the mail server.

A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

18. Click **OK**.

The **Call Home Configuration** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

19. Click **OK** to close the **Call Home Configuration** dialog box.

## Editing the EMC call home center

To edit an EMC call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select the **EMC** call home center you want to edit in the **Call Home Centers** table.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).

The **Configure Call Home Center** dialog box displays ([Figure 52](#)).

**FIGURE 52** Configure Call Home Center dialog box (EMC option)

4. Make sure the **EMC** call home center type displays in the **Call Home Centers** list.
5. Select **Enable** to enable this call home center.
6. Set the time interval at which to check the call home center by selecting the **Set the heartbeat interval at \_\_\_ days (1-28)** check box and entering the interval in the field.

## 4 Editing the HP LAN call home center

7. Enter the phone number or extension of the local server in the **Local Server - Modem #** field.
8. Enter the identification number of the local server in the **Local Server - Cabinet Serial #** field.
9. Enter the site name for the local server in the **Local Server - Site Name** field.
10. Click **Send Test** to test the Connect EMC application.

The selected call home center must be enabled to test the Connect EMC application.

A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

11. Click **OK**.

The **Call Home** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

12. Click **OK** to close the **Call Home** dialog box.

### Editing the HP LAN call home center

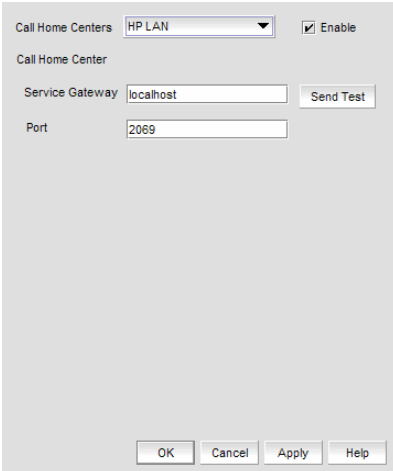
To edit an HP LAN call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select the **HP LAN** call home center you want to edit in the **Call Home Centers** table.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).

The **Configure Call Home Center** dialog box displays ([Figure 53](#)).



**FIGURE 53** Configure Call Home Center dialog box (HP LAN option)

4. Make sure the **HP LAN** call home center type displays in the **Call Home Centers** list.
5. Select **Enable** to enable this call home center.
6. Enter the IP address of the call home center in the **Service Gateway** field.
7. Enter the port number (default is 2069) of the call home center in the **Port** field

8. Click **Send Test** to test the address.

The selected call home center must be enabled to test the IP address.

A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

---

**NOTE**

The HP LAN Call Home alert displays the directory separation characters with a double backslash (\\) instead of a single backslash (\).

---

9. Click **OK**.

The **Call Home** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

10. Click **OK** to close the **Call Home** dialog box.

## Enabling a call home center

To enable a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select the **Enable** check box of the call home center you want to enable in the **Call Home Centers** table.
3. Click **OK** to close the **Call Home** dialog box.

## Enabling support save

---

**NOTE**

Only supported on Fabric OS switches with firmware 5.2 or later.

---

When you enable Support Save through the call home center, all call home events trigger the Support Save operation and the Support Save stored location on the FTP server is transmitted with the call home event.

To enable a support save for a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select the **Support Save** check box of the call home center for which you want to enable support save in the **Call Home Centers** table.
3. Click **OK** to close the **Call Home** dialog box.

### Testing the call home center connection

Once you add and enable a call home center, you should verify that call home is functional.

To verify call home center functionality, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.
2. Click **Edit Centers** (beneath the **Call Home Centers** table).  
The **Configure Call Home Center** dialog box displays.
3. Select the center you want to check in the **Call Home Centers** list.
4. Make sure that the **Enabled** check box is selected.

---

#### NOTE

You must configure the call home center before you test the connection. To configure a call home center, refer to [“Editing a call home center”](#) on page 109.

---

5. Click **Send Test**.  
A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.
6. Click **OK** to close the ‘Test Event Sent’ message.
7. Click **OK** to close the **Configure Call Home Center** dialog box.
8. Click **OK** to close the **Call Home** dialog box.

### Disabling a call home center

When a call home center is disabled, no devices can send call home events to the call home center. However, the devices and event filters assigned to the disabled call home center are not removed. You can still perform the following actions on a disabled call home center:

- Edit call home center configuration.
- Add devices and event filters to the call home center.

To disable a call home center, complete the following steps.




1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Clear the **Enable** check box of the call home center you want to disable in the **Call Home Centers** table.  
The selected call home center and its devices and event filters become grayed out. However, the call home center is not actually disabled until you save your changes. When a device is assigned to the call home center, a confirmation message displays.
3. Click **OK** to confirm.
4. Click **OK** to close the **Call Home** dialog box.

## Viewing Call Home status

You can view call home status from the main Management application window or from the **Call Home Notification** dialog box.

The Management application enables you to view the call home status at a glance by providing a call home status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the call home function.

**TABLE 8** Call Home Icons

Icon	Description
	Normal— Displays when call home is enabled on all devices and no filters are applied.
	Degraded— Displays when call home is enabled on all devices and at least one filter is active.
	Disabled— Displays when any of the following conditions are met: <ul style="list-style-type: none"> <li>• At least one device's call home is disabled.</li> <li>• At least one non-manageable switch.</li> <li>• At least one switch does not have the Management server registered as a trap recipient.</li> </ul>

To view more detail regarding call home status, click the **Call Home** icon. The **Call Home Notification** dialog box displays the list of devices that have assigned filters or call home disabled.

The following table explains the statuses that may be displayed in the **Call Home Notification** dialog box.

**TABLE 9** Call Home Status

Status	Description
Enabled	The device is manageable, call home is enabled, and a filter is applied.
Disabled	Call home is disabled on at least one device or call home is disabled from the <b>Call Home</b> dialog box.
Not Manageable	Manageability is lost.
Server Not Registered	The Server is not registered to receive Call Home events from this device. <b>Note:</b> Fabric OS switches only.

### Assigning a device to the call home center

Discovered devices (switches, routers, and directors) are not assigned to a corresponding call home center automatically. You must manually assign each device to a call home center before you use call home.

To assign a device or multiple devices to a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select the devices you want to assign to a call home center in the **Products List** table.
3. Select the call home center to which you want to assign the devices in the **Call Home Center** table.

You can only assign a device to one call home center at a time.

If you do not select a call home center, the selection defaults to the first call home center in the **Call Home Center** table.

If you have made a previous selection on an assigned device or filter and you do not select a call home center, the selection defaults to the previous selection's call home center.

4. Click the right arrow button.

The selected devices display beneath the selected call home center. Devices assigned to a call home center do not display in the **Products List** table.

5. Click **OK** to close the **Call Home** dialog box.

### Removing a device from a call home center

To remove a device or multiple devices from a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select the call home center from which you want to remove devices in the **Call Home Center** table.

3. Select the devices you want to remove from the selected call home center.

4. Click the left arrow button.

A confirmation message displays.

5. Click **OK**.

The selected devices are removed from the call home center and display in the **Products List** table.

6. Click **OK** to close the **Call Home** dialog box.

## Removing all devices and filters from a call home center

To remove all devices and filters from a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Select the call home center from which you want to remove devices and filters in the **Call Home Center** table.
3. Click the left arrow button.  
A confirmation message displays.
4. Click **OK**.  
All devices assigned to the selected call home center display in the **Products List** table. Any assigned filters are also removed.
5. Click **OK** to close the **Call Home** dialog box.

## Defining an event filter

To define an event filter, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Click **Add** beneath the **Call Home Event Filter** table.  
The **Call Home Event Filter** dialog box displays.
3. Enter a name for the filter in the **Name** field.
4. Enter a name for the description in the **Description** field.
5. Select the events you want to include in the filter in the **Available Call Home Event Types** table.  
Click **Select All** to select all event types in the table or select **Unselect All** to clear the selected event types in the table. For more information about Call Home events, refer to [Appendix B, "Call Home Event Tables"](#).
6. Click **OK**.  
The Event Filter name and the description are displayed in the **Call Home** dialog box.
7. Click **OK** to close the **Call Home** dialog box.  
To assign event filters to a call home center or a device, refer to ["Assigning an event filter to a call home center"](#) on page 120 or ["Assigning an event filter to a device"](#) on page 120.

## Call Home for virtual switches

For virtual switches, there are two types of Call Home events:

- FRU-based Call Home events which are triggered at the chassis level.
- Port-based Call Home events, which are triggered for each virtual switch.

## Assigning an event filter to a call home center

Event filters allow call home center users to log in to a Management server and assign specific event filters to the devices. This limits the number of unnecessary or 'acknowledge' events and improves the performance and effectiveness of the call home center.

You can only select one event filter at a time; however, you can assign the same event filter to multiple devices or call home centers. When you assign an event filter to a call home center, the event filter is assigned to all devices in the call home center. For more information about Call Home events, refer to [Appendix B, "Call Home Event Tables"](#).

---

### NOTE

You cannot assign an event filter to a call home center that does not contain devices.

---

To assign an event filter to a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Select the event filters you want to assign in the **Call Home Event Filters** table.
3. Select the call home centers to which you want to assign the event filters in the **Call Home Centers** table.
4. Click the right arrow button.  
The selected event filters are assigned to the selected call home centers.
5. Click **OK** to close the **Call Home** dialog box.

## Assigning an event filter to a device

To assign an event filter to a device, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Select the event filter you want to assign in the **Call Home Event Filters** table.  
For more information about Call Home events, refer to [Appendix B, "Call Home Event Tables"](#).
3. Select one or more devices to which you want to assign the event filter in the **Call Home Centers** table.
4. Click the right arrow button.  
The selected event filter is assigned to the selected devices. The event filter displays beneath the specified device or all of the devices under the specified call home center.
5. Click **OK** to close the **Call Home** dialog box.

## Overwriting an assigned event filter

A device can only have one event filter at a time; therefore, when a new filter is applied to a device that already has a filter, you must confirm the new filter assignment.

To overwrite an event filter, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Select the event filter you want to apply in the **Call Home Event Filters** table.

For more information about Call Home events, refer to [Appendix B, “Call Home Event Tables”](#).

3. Select the devices to which you want to apply the event filter in the **Call Home Centers** table.

4. Click the right arrow button.

For existing event filters, a confirmation messages displays.

5. Click **Yes**.

The selected event filter is applied to the selected devices. The event filter displays beneath the specified device or all of the devices under the specified call home center.

6. Click **OK** to close the **Call Home** dialog box.

## Removing an event filter from a call home center

To remove all event filters from a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

The **Call Home** dialog box displays.

2. Choose one of the following options in the **Call Home Centers** table:

- Right-click a call home center and select **Remove Filters**.
- Select the call home center and click the left arrow button.

All event filters assigned to the call home center are removed.

3. Click **OK** to close the **Call Home** dialog box.

### Removing an event filter from a device

To remove an event filter from a device, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Choose one of the following options in the **Call Home Centers** table:
  - Right-click an event filter assigned to a device and select **Remove Filter**.
  - Right-click a device to which the event filter is assigned and select **Remove Filter**.
  - Select an event filter assigned to a device and click the left arrow button. Press **CTRL** and click to select multiple event filters assigned to multiple devices.  
All event filters assigned to the device are removed.
3. Click **OK** to close the **Call Home** dialog box.

### Removing an event filter from the Call Home Event Filters table

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Select the event filter you want to remove in the **Call Home Event Filters** table.
3. Click **Remove**.
  - If the event filter is not assigned to any devices, a confirmation message displays asking if you want to remove the event filter. Click **Yes**.
  - If the event filter is assigned to any devices, a confirmation message displays informing you that removing this event filter will remove it from all associated devices. Click **Yes**.  
The event filter is removed from any associated devices and the **Call Home Event Filters** table.  
To determine to which devices the event filter is assigned, select the event filter and then click the find button (>).
4. Click **OK** to close the **Call Home** dialog box.

### Searching for an assigned Event Filter

To find all devices to which an event filter is assigned, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.  
The **Call Home** dialog box displays.
2. Select the event filter you want to find in the **Call Home Event Filters** table.
3. Click > (find button).
4. All instances of the event filter are highlighted in the **Call Home Centers** table.  
If the selected event filter is not assigned to any devices in the **Call Home Centers** table, a not found message displays.

# View management

---

## In this chapter

• About view management .....	123
• Creating a customized view .....	124
• Editing a customized view .....	125
• Deleting a customized view .....	126
• Copying a view .....	127
• About topology layout .....	127
• Customizing the layout of devices on the topology .....	128
• Customizing the layout of connections on the topology .....	129
• Changing a group's background color .....	129
• Reverting to the default background color .....	130
• Changing the product label .....	131
• Changing the port label .....	131
• Changing the port display .....	131
• Grouping on the topology .....	132

## About view management

You can customize the topology by creating views that include certain fabrics or devices and then switch between the views to see specific information about those fabrics or devices.

If you discover or import a Fabric with more than approximately 2000 devices, the devices display on the Product List, but not on the Connectivity Map. Instead, the topology area shows a message stating that the topology cannot be displayed. To resolve this issue, create a new view to filter the number of devices being discovered. Refer to [Creating a customized view](#) for instructions.

Creating a customized view

You may want to customize the Product List and Connectivity Map to simplify management of large SANs by limiting the topology size or Product List columns.

For each customized view, you can specify the fabrics and hosts that display on the Connectivity Map as well as the columns and device groupings that display on the Product List.

Customized view settings reside on the Server. Only users with the same login to the same Server can see and select the view settings. No individual user can have access to the views created by another user.

If you select a customized view and new devices are discovered, those new devices display in the customized view if they belong in that view category or fabric.

1. Use one of the following methods to open the **Create View** dialog box:
- Select **View > Manage View > Create View**.

Select **Create View** from the **View All** list. Does not display until you discover a fabric.

The **Create View** dialog box displays (Figure 54).

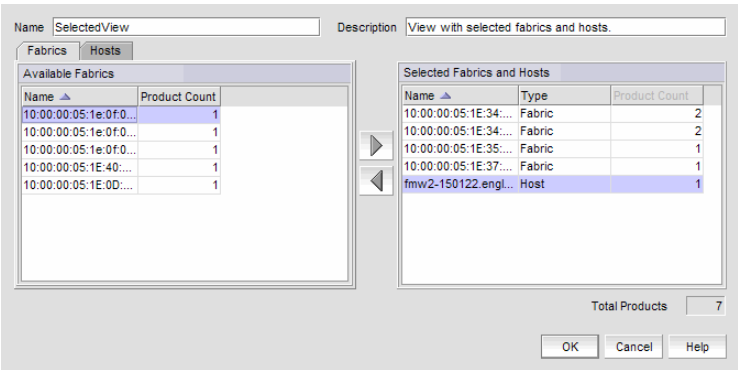


FIGURE 54 Create View dialog box - Fabrics Tab

2. Enter a name (128 character maximum) and a description (126 character maximum) for the view.

NOTE

You cannot use the name View or View All.

NOTE

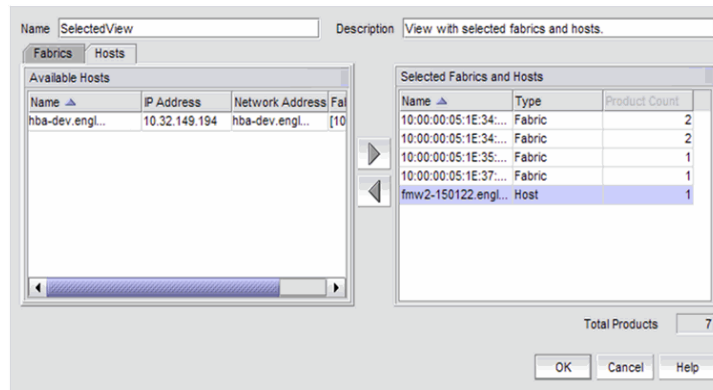
You cannot use an existing name.

3. In the **Available Fabrics** table, select the fabrics you want to include in the view and use the right arrow button to move your selections to the **Selected Fabrics and Hosts** table.

NOTE

Use *CTRL* + *click* to select more than one individual row or *SHIFT* + *click* to select multiple rows sequentially.

- Click the **Hosts** tab and in the **Available Host** table, select the fabrics you want to include in the view and use the right arrow button to move your selections to the **Selected Fabrics and Hosts** table.



**FIGURE 55** Create View dialog box - Hosts Tab

- Click **OK** to save the customized view and close the **Create View** dialog box.  
The new view displays automatically in the main window of the Management application.

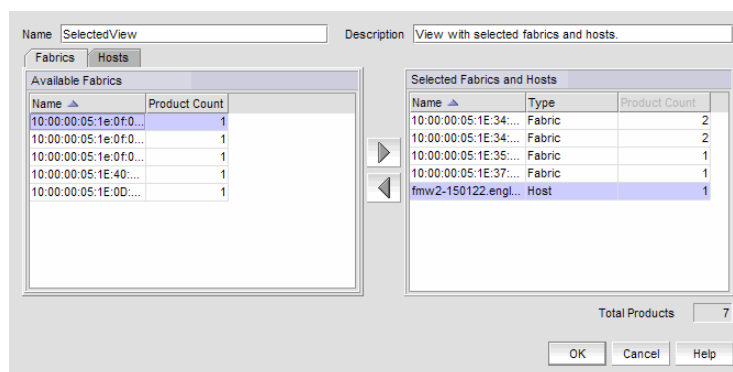
## Editing a customized view

You may only edit customized views that you have created.

Customized view settings reside on the Server. Only users with the same login to the same Server can see and edit the view settings. No individual user can have access to the views created by another user.

- Use one of the following methods to open the **Edit View** dialog box:
  - Select **View > Manage View > Edit View > View\_Name**.
  - Select **Edit View** from the **View All** list. Does not display until you discover a fabric.

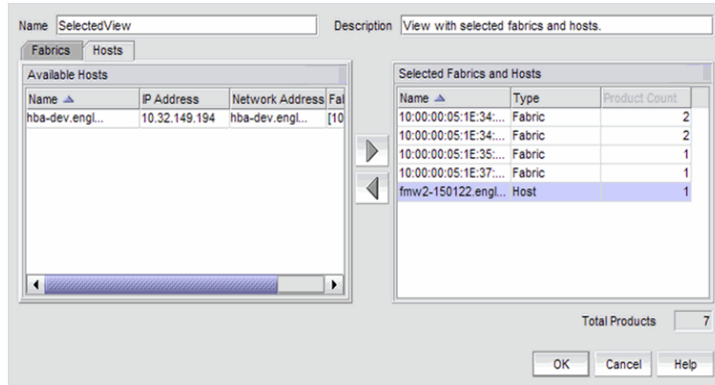
The **Edit View** dialog box displays.



**FIGURE 56** Edit View dialog box - Fabrics Tab

## 5 Deleting a customized view

2. Use the left arrow button to remove fabrics and hosts from the **Selected Fabrics and Hosts** table.
3. Click the **Fabrics** tab, and in the **Available Fabrics** table, select the fabrics you want to include in the view and use the right arrow button to move your selections to the **Selected Fabrics and Hosts** table.
4. Click the **Hosts** tab and in the **Available Host** table, select the fabrics you want to include in the view and use the right arrow button to move your selections to the **Selected Fabrics and Hosts** table.



**FIGURE 57** Edit View dialog box - Hosts Tab

5. Click **OK** to save your changes and close the **Edit View** dialog box.
6. Verify your changes on the main window.

## Deleting a customized view

Customized view settings reside on the Server. No individual user has access to the views created by another user and therefore cannot delete another user's view.

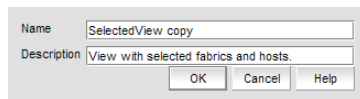
To delete a customized view, use the following procedure.

1. Select **View > Manage View > Delete View > View\_Name**.
2. Click **Yes** on the message.

## Copying a view

1. Use one of the following methods to open the **Copy View** dialog box:
  - Select **View > Manage View > Copy View > View\_Name**.
  - Select **Copy View** from the **View All** list. Does not display until you discover a fabric.

The **Copy View** dialog box title displays the name of the view you are copying.



**FIGURE 58** Copy View dialog box

2. Enter a name and description of the view.
3. Click **OK** to save your changes and close the **Copy View** dialog box.
4. Verify that the copied view displays on the main window.

## About topology layout

This section provides an overview of topology layout options and instructions for changing the layout. You can customize various parts of the topology, including the layout of devices and connections as well as groups' background colors, to easily and quickly view and monitor devices in your SAN.

The following menu options are available on the **View** menu. Use these options to customize the topology layout.

**Map Display.** Select to specify a new layout for the desktop icons, background color for groups, as well as line type for connections between icons.

**Domain ID/Port #.** Select to set the display domain IDs and port numbers in decimal or hex format.

**Decimal.** Select to display all domain IDs and port numbers in decimal format.

**Hex.** Select to display all domain IDs and port indexes (user port #) in hex format.

**Product Label.** Select to configure which product labels display.

---

### NOTE

Changes apply to all fabrics present in the topology when the **Product Label** option is selected.

---

**Name (Product).** Displays the product name as the product label.

**WWN.** Displays the world wide name as the product label.

**IP Address.** Displays the IP Address as the product label.

**Domain ID.** Displays the domain ID as the product label.

**Port Label.** Select to configure which port labels display.

---

### NOTE

Changes apply to the selected fabric or the fabric to which the selected item belongs.

---

**Name.** Displays the name as the port label. If the port has not been given a name, the port's WWN displays.

**Port Number.** Displays the port number as the port label.

**Port Address.** Displays the port address as the port label.

**Port WWN.** Displays the port world wide name as the port label.

**User Port #.** Displays the user's port number as the port label.

**Slot/Port.** Displays the slot and port as the port label for a Chassis switch and the port number for a switch.

**Port Display.** Select to configure how ports display.

**Occupied Product Ports.** Select to display the ports of the devices in the fabrics (present in the connectivity map) that are connected to other devices.

**UnOccupied Product Ports.** Select to display the ports of the devices (shown in the connectivity map) that are not connected to any other device.

**Attached Ports.** Select to display the attached ports of the target devices.

**Switch to Switch Connections.** Select to display the switch to switch connections. Switch to switch connections only display when the **Attached Ports** option is also selected.

## Customizing the layout of devices on the topology

You can customize the layout of devices by group type or for the entire Connectivity Map. Customizing the layout makes it easier to view the SAN and manage its devices. Group types include Fabric, Host, Storage, and Switch groups. The **Map Display Layout** list varies depending on what you selected (group type or Connectivity Map).

1. Right-click a group or the Connectivity Map and select **Map Display**, then select one of the following options:
  - **Default for Group\_Type.** Displays the devices in the default format. Group types include Fabric, Host, Storage, and Switch groups.
  - **Free Form.** Displays the devices in the default format for Switch Groups and Router Groups.  
When the **Free Form** map display layout is selected, the **Show Ports** menu command is unavailable.
  - **Fabric.** Displays the devices in the default format.
  - **Custom Grid.** Enables you to drag and drop product or group icons into a variable grid to reorganize the topology. The grid prevents icons from obscuring other icons. If enabled on a group, devices can only be moved within the group. If enabled on a fabric, groups can only be moved within the fabric. In other words, a device cannot be moved outside of its group.
  - **Square.** Displays the device icons in a square configuration.

- **Vertical.** Displays the device icons vertically.
  - **Horizontal.** Displays the device icons horizontally.
  - **Most Connected at Center.** Displays the node that has the most connections at the center of the topology.
  - **Directional.** Displays the internal nodes in a position where they mirror the external groups to which they are connected.
2. Select the **Set as Default Layout** check box to set your selection as the default.
  3. Click **OK** on the **Map Display Properties** dialog box.

## Customizing the layout of connections on the topology

You can change the way inter-device connections display on the topology.

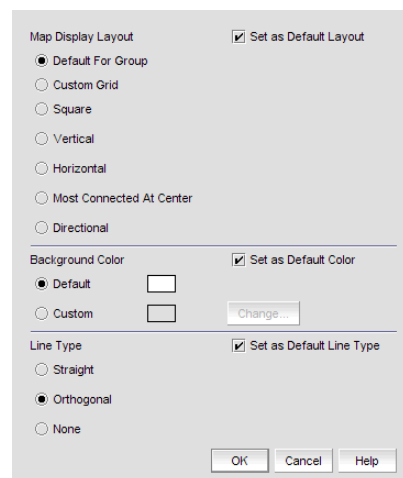
1. Right-click a group or the Connectivity Map and select **Map Display**, then select one of the following options:
  - **Straight.** Displays connections using straight lines.
  - **Orthogonal.** Displays connections in orthogonal grid lines. Disabled if **Free Form** is selected in **Map Display Layout** area.
  - **None.** Hides the connections between devices.
2. Select the **Set as Default Layout** check box to set your selection as the default.
3. Click **OK** on the **Map Display Properties** dialog box.

## Changing a group's background color

You can customize the topology by changing a group's background color.

1. Right-click a group or the Connectivity Map and select **Map Display**.

The **Map Display Properties** dialog box displays (Figure 59).

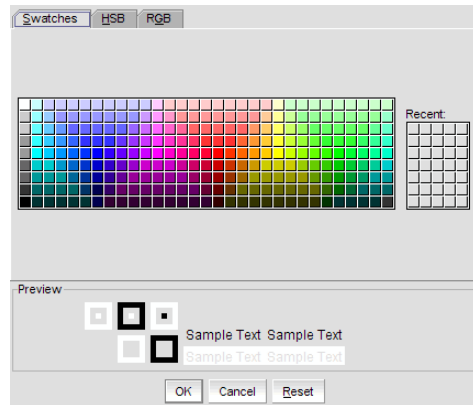


**FIGURE 59** Map Display dialog box

## 5 Reverting to the default background color

2. Select the **Custom** option and click **Change**.

The **Choose a background color** dialog box displays (Figure 60).



**FIGURE 60** Map Display dialog box

3. Select or specify a color and preview it in the **Preview** pane.
  - To pick a color from a swatch, select the **Swatches** tab. Select a color from the display.
  - To specify a color based on hue, saturation, and brightness, click the **HSB** tab. Specify the hue (0 to 359 degrees), saturation (0 to 100%) and brightness (0 to 100%).
  - To specify a color based on values of red, green, and blue, click the **RGB** tab. Specify the values for red, green, and blue (0 to 255).
4. Click **OK** to change the background color, or click **Reset** to return all settings to the color currently being displayed on the topology.
5. Click **OK** on the **Map Display Properties** dialog box.

## Reverting to the default background color

You can revert back to the default background color.

1. Right-click a group and select **Map Display**.

The **Map Display Properties** dialog box displays.
2. Select the **Default** option.
3. Click **OK** on the **Map Display Properties** dialog box.

## Changing the product label

1. Select a product in the Connectivity Map or Product List.
2. Select **View > Product Label**, then select one of the following options:
  - **Name (Product)**. Displays the product name as the product label.
  - **WWN**. Displays the world wide name as the product label.
  - **IP Address**. Displays the IP Address as the product label.
  - **Domain ID**. Displays the domain ID as the product label.

Changes apply to all fabrics present in the topology when the **Product Label** option is selected.

## Changing the port label

1. Select a port in the Connectivity Map or Product List.
2. Select **View > Port Label**, then select one of the following options:
  - **Name**. Displays the name as the port label.
  - **Port Number**. Displays the port number as the port label.
  - **Port Address**. Displays the port address as the port label.
  - **Port WWN**. Displays the port world wide name as the port label.
  - **User Port #**. Displays the user's port number as the port label.
  - **Slot/Port**. Displays the slot and port as the port label.

All port labels within the fabric to which the selected item belongs change to the selected port label type.

## Changing the port display

You have the option of viewing connected (or occupied) product ports, unoccupied product ports, or attached ports.

---

**NOTE**

Occupied/connected ports are those that originate from a device, such as a switch. Attached ports are ports of the target devices that are connected to the originating device.

---

Select **View > Port Display**, then select one or more of the following options:

- **Occupied Product Ports**. Displays the ports of the devices in the fabrics (present in the connectivity map) that are connected to other devices.
- **Unoccupied Product Ports**. Displays the ports of the devices (shown in the connectivity map) that are not connected to any other device.
- **Attached Ports**. Displays the attached ports of the target devices.
- **Switch to Switch Connections**. Displays the connections between devices. Switch to switch connections only display when the **Attached Ports** option is also selected.


All port labels on all fabrics change to the selected port label type.

## Grouping on the topology

To simplify management, devices display in groups. Groups are shown with background shading and are labeled appropriately. You can expand and collapse groups to easily view a large topology.

### Collapsing groups

To collapse a single group on the topology, do one of the following:

- Click the icon at the top right-hand corner of the group on the topology ().
- Double-click in the group, but not on a device.
- Right-click in a group, but not on a device, and select **Collapse** from the shortcut menu.

To collapse all groups on the topology by one level, click the **Collapse** button on the toolbox (.

### Expanding groups

To expand a group on the topology, do one of the following:

- Double-click on the group icon.
- Right-click the group icon and select **Expand** from the shortcut menu.

To expand all groups on the topology by one level, click the **Expand** button on the toolbox (.

### Viewing connections

You can view the connections in a fabric using one of the following methods:

- Select a fabric and then select **View > Connected End Devices** and select **Include Virtual Devices**, **Hide All**, **Show All**, or **Custom**.
- Right-click on the fabric and select **Connected End Devices > Include Virtual Devices**, **Hide All**, **Show All**, or **Custom**.

### Configuring custom connections

---

#### NOTE

Active zones must be available on the fabric.

---

To create a display of the connected end devices participating in a single zone or group of zones, complete the following steps.

1. Choose from one of the following options:
  - Select a fabric on the topology and select **View > Connected End Devices > Custom**.
  - Right-click a fabric on the topology and select **Connected End Devices > Custom**.

The **Connected End Devices - Custom display for Fabric** dialog box displays with a list of zones in the **Zones in Fabric** list.

2. Select the zones you want to include in the connection in the **Zones in Fabric** list.
3. Select the application you want to add the selected zones to in the **Application** list.

4. Click the right arrow to move them to the **Selected Zones** list.
5. Click **OK**.

## Saving a custom connection configuration

---

**NOTE**

Active zones must be available on the fabric.

---

To save a new custom connection configuration, complete the following steps.

1. Choose from one of the following options:
  - Select a fabric on the topology and select **View > Connected End Devices > Custom**.
  - Right-click a fabric on the topology and select **Connected End Devices > Custom**.The **Connected End Devices - Custom display for Fabric** dialog box displays with a list of zones in the **Zones in Fabric** list.
2. Select the zones you want to include in the connection in the **Zones in Fabric** list.
3. Click the right arrow to move the selected zones to the **Selected Zones** list.
4. Click **Save**.

The **Save Application** dialog box displays.
5. Enter a new name in the **Application Name** field.
6. Click **OK** on the **Save Application** dialog box.
7. Click **OK** on the **Connected End Devices - Custom display for Fabric** dialog box.

The saved custom connection configuration displays in the **Connected End Devices** menu.

## Deleting a custom connection configuration

---

**NOTE**

Active zones must be available on the fabric.

---

To delete a custom connection configuration, complete the following steps.

1. Choose from one of the following options:
  - Select a fabric on the topology and select **View > Connected End Devices > Custom**.
  - Right-click a fabric on the topology and select **Connected End Devices > Custom**.The **Connected End Devices - Custom display for Fabric** dialog box.
2. Select the configuration you want to delete in the **Application** list.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Click **OK** on the **Connected End Devices - Custom display for Fabric** dialog box.

## Customizing the main window

You can customize the main window to display only the data you need by displaying different levels of detail on the Connectivity Map (topology) or Product List.

### Zooming in and out of the connectivity map

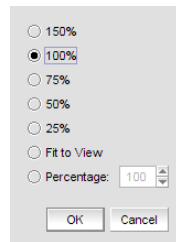
You can zoom in or out of the Connectivity Map to see products and ports.

#### *Zooming In*

To zoom in on the Connectivity Map, use one of the following methods:

- Click the zoom-in icon (🔍) on the toolbox.
- Press CTRL + NumPad+ on the keyboard.
- Use the **Zoom** dialog box.
  - a. Select **View > Zoom**.

The **Zoom** dialog box displays (Figure 61).



**FIGURE 61** Zoom dialog box

- b. Select a zoom percentage.
- c. Click **OK** to save your changes and close the **Zoom** dialog box.

#### *Zooming out*

To zoom out of the Connectivity Map, use one of the following methods:

- Click the zoom-out icon (🔍) on the toolbox.
- Press CTRL + NumPad- on the keyboard.
- Use the **Zoom** dialog box.
  - a. Select **View > Zoom**.

The **Zoom** dialog box displays.

- b. Select a zoom percentage.
- c. Click **OK** to save your changes and close the **Zoom** dialog box.

## Showing levels of detail on the connectivity map

You can configure different levels of detail on the Connectivity Map, making Management easier.

### *View Fabrics*

To view only fabrics, without seeing groups, products or ports:

Select **View > Show> Fabrics Only**.

### *View Groups*

To view only groups and fabrics, without seeing products or ports:

Select **View > Show> Groups Only**.

### *View Products*

To view products, groups, and fabrics:

Select **View > Show> All Products**.

### *View Ports*

To view all ports:

Select **View > Show> All Ports**.

## Exporting the topology

You can save the topology to a image (PNG format).

1. Click **Export** in the tool box.

The **Export Topology To PNG File** dialog box.

2. Browse to the directory where you want to export the image.
3. Edit the name in the **File Name** field, if necessary.
4. Click **Save**.

If the file name is a duplicate, a message displays. Click **Yes** to replace the image or click **No** to go back to the **Export Topology To PNG File** dialog box and change the file name.

The **File Download** dialog box displays.

5. Click **Open** to view the image or click **Cancel** to close the dialog box.

## Customizing application tables

You can customize any table in the Management application (for example, the Master Log or the Product List) in the following ways:

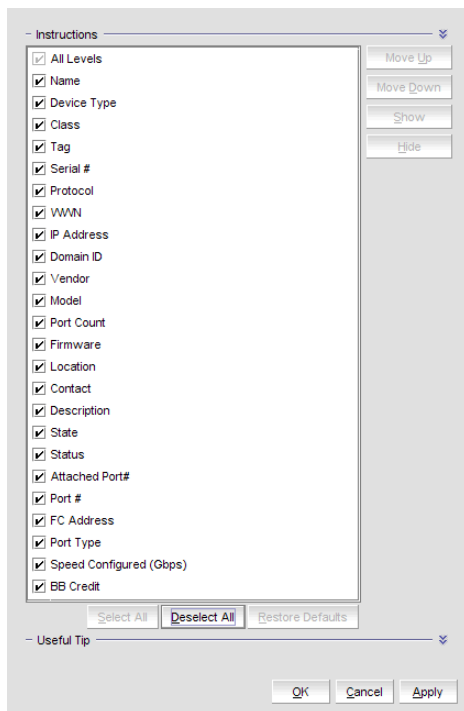
- Display only specific columns
- Display columns in a specific order
- Resize the columns to fit the contents
- Sort the table by a specific column or multiple columns
- Copy information from the table to another application
- Export information from the table
- Search for information
- Expand the table to view all information
- Collapse the table

### Displaying columns

To only display specific columns, complete the following steps.

1. Right-click anywhere in the table and select **Customize** or **Table > Customize**.

The **Customize Columns** dialog box displays.



**FIGURE 62** Customize Columns dialog box

2. Choose from the following options:
  - Select the check box to display a column.  
OR  
Select the column name and click **Show**.
  - Clear the check box to hide a column.  
OR  
Select the column name and click **Hide**.
  - Click **Select All** to select all check boxes.
  - Click **Deselect All** to clear all check boxes.
  - Click **Restore Defaults** to restore the Product List to the original settings.
3. Click **OK**.

### *Changing the order of columns*

To change the order in which columns display, choose from one of the following options.

Rearrange columns in a table by dragging and dropping the column to a new location.

OR

1. Right-click anywhere in the table and select **Customize** or **Table > Customize**.  
The **Customize Columns** dialog box displays.
2. Highlight the name of the column you want to move and use **Move Up** and **Move Down** to move it to a new location.
3. Click **OK**.

### *Resizing the columns*

You can resize a single column or all columns in the table.

To resize a single column, right-click the column header and select **Size Column to Fit** or **Table > Size Column to Fit**.

To resize all columns in the table, right-click anywhere in the table and select **Size All Columns to Fit** or **Table > Size All Columns to Fit**.

### *Sorting table information*

To sort the product list by a single column, click the column header.

To reverse the sort order, click the column header again.

To sort the product list by multiple columns, complete the following steps.

1. Click the primary column header.
2. Press CTRL and click a secondary column header.

## Copying table information

You can copy the entire table or a specific row to another application (such as, Notepad, Excel, Word, and so on).

1. Choose from one of the following options:
  - Right-click anywhere in the table and select **Table > Copy Table**.
  - Select the table row that you want to export and select **Table > Copy Row**.
2. Open the application to which you want to copy the Product List information.
3. Select **Edit > Paste** or **CTRL + V**.
4. Save the file.

## Exporting table information

You can export the entire table or a specific row to a text file.

1. Choose from one of the following options:
  - Right-click anywhere in the table and select **Table > Export Table**.
  - Select the table row that you want to export and select **Table > Export Row**.

The **Save table to a tab delimited file** dialog box displays.

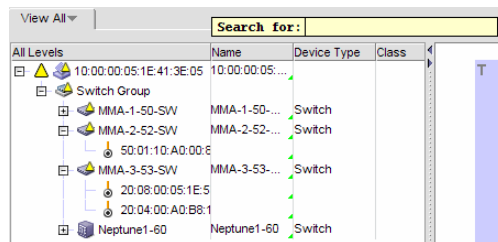
2. Browse to the location where you want to save the file.
3. Enter file name in the **File Name** field.
4. Click **Save**.

## Searching for information in a table

You can search for information in the table by any of the values found in the table.

1. Right-click anywhere in the table and select **Table > Search**.

The **Search for** field displays.



**FIGURE 63** Search for field

2. Enter all or part of the search text in the **Search for** field.  
The first instance is highlighted in the table.
3. Press **Enter** to go to the next instance of the search text.

### *Expanding and collapsing tables*

You can expand a table to display all information or collapse it to show only the top level.

To expand the entire table, right-click anywhere in the table and select **Expand All** or **Table > Expand All**.

To collapse the entire table, right-click anywhere in the table and select **Collapse All** or **Table > Collapse All**.

## Searching for a device in the connectivity map

You can search for a device in the connectivity map by name, WWN, or device type. When searching in the connectivity map, make sure you search the right view (**View > Manage View > Display View > View\_Name**) with the appropriate options of port display (**View > Port Display > Display\_Option**) and connected end devices (**View > Port Display > Show All**) enabled.

1. Enter all or part of the device type, name, or WWN in the search field.

---

**NOTE**

To search for a device, the device must be discovered and display in the topology.

---

2. Press **Enter** or click **Search**.

## 5 Searching for a device in the connectivity map

# Third-party tools

---

## In this chapter

• About third-party tools.....	141
• Starting third-party tools from the application .....	142
• Launching a Telnet session .....	142
• Launching an Element Manager .....	143
• Launching Web Tools.....	143
• Launching FCR configuration .....	144
• Launching HCM Agent.....	145
• Adding a tool .....	146
• Entering the server IP address of a tool.....	147
• Adding an option to the Tools menu.....	147
• Changing an option on the Tools menu .....	149
• Removing an option from the Tools menu.....	149
• Changing an option on a device's shortcut menu.....	151
• Removing an option from a device's shortcut menu .....	152
• VMware vCenter plug-in .....	153

## About third-party tools

You can add third-party tools to the **Tools** menu or shortcut menus to open other software products (such as, Firefox, Windows Explorer, Web Tools, Element Managers, FCR Configuration, HCM Agent and so on) you frequently use.

## Starting third-party tools from the application

You can open third-party tools from the **Tools** menu or a device's shortcut menu. Remember that you cannot open a tool that is not installed on your computer. You must install the tool on your computer and add the tool to the **Tools** menu or the device's shortcut menu.

To open an application, perform the following steps.

1. Select the device.
2. Use one of the following techniques:
  - Select **Tools > Product Menu > Tool\_Name**.
  - Select **Tools > Tool\_Name**.
  - Right-click the device, and select the tool from the menu.

If the third-party tool is a web-based application, you must enter the IP address of the applications server as a parameter to be able to open the application. For step-by-step instructions about entering the IP address of the server, refer to [“Entering the server IP address of a tool”](#) on page 147.

## Launching a Telnet session

You can use Telnet to log in and issue command line-based commands to a switch.

---

**NOTE**

The switch must have a valid IP address. If the device does not have a valid IP address, the Telnet selection will not be available on the **Tools** menu or the shortcut menu. You must right-click the device icon, select **Properties**, and enter the device's IP address before you can open a Telnet session.

---

To launch a telnet session, complete the following steps.

On the Connectivity Map, right-click a device and select **Telnet** or **Telnet through Server**.

---

**NOTE**

Telnet through Server is only supported on Windows systems.

---

OR

1. Select the switch to which you want to connect.
2. Select **Tools > Product Menu > Telnet**.

The Telnet session window displays.

---

**NOTE**

On Linux systems, you must use CTRL + BACKSPACE to delete text in the Telnet session window.

---

## Launching an Element Manager

Element Managers are used to manage Fibre Channel switches and directors. You can open a device's Element Manager directly from the application.

To launch a device's Element Manager, complete the following steps.

On the Connectivity Map, double-click the device you want to manage.

The Element Manager displays.

OR

On the Connectivity Map, right-click the device you want to manage and select **Element Manager > Hardware**.

The Element Manager displays.

OR

1. Select a device.
2. Select **Configure > Element Manager > Hardware**.

The Element Manager displays.

OR

1. Select a device.
2. Click the Element Manager icon on the toolbar.

The Element Manager displays.

## Launching Web Tools

Use Brocade Web Tools to enable and manage Brocade Access Gateway, Switches, and Directors. You can open Web Tools directly from the application. For more information about Web Tools, refer to the *Brocade Web Tools Administrator's Guide*. For more information about Brocade Access Gateway, Switches, and Directors, refer to the documentation for the specific device.

To launch a device's Element Manager, complete the following steps.

---

### NOTE

You must have Device Administration privileges for the selected device to launch Web Tools. If you do not have Device Administration privileges, you will need to enter those credentials to launch Web Tools.

---

On the Connectivity Map, double-click the Fabric OS device you want to manage.

Web Tools displays.

OR

On the Connectivity Map, right-click the Fabric OS device you want to manage and select **Element Manager > Hardware**.

Web Tools displays.

OR

1. Select a Fabric OS device.
2. Select **Configure > Element Manager > Hardware**.

Web Tools displays.

OR

1. Select a Fabric OS device.
2. Click the Element Manager icon on the toolbar.

Web Tools displays.

## Launching FCR configuration

Use FCR Configuration to launch the FC Routing module, which enables you to share devices between fabrics without merging the fabrics. You can open the FC Routing module directly from the Management application. For more information about FC Routing, refer to the *Brocade Web Tools Administrator's Guide*.

The FCR Configuration option is available only for the following devices with Fabric OS 5.0 or later:

- Fabric OS extension switch
- Fabric OS Directors configured with an extension blade
- Fabric OS 1U, 40-port, 8 Gbps FC Switch (with Integrated Routing license)
- Fabric OS 2U, 80-port, 8 Gbps FC Switch (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 16-port Blade (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 32-port Blade (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 48-port Blade (with Integrated Routing license)

Note that on the FC 8 GB 48-port Blade, the Shared Area ports, for example, 16-47, cannot be configured as EX\_ports

On the Connectivity Map, right-click the Fabric OS device you want to configure and select **Element Manager > Router Admin**.

OR

1. Select a Fabric OS device.
2. Select **Configure > Element Manager > Router Admin**.

The FC Routing module displays.

## Launching HCM Agent

Use Brocade HCM Agent to enable and manage Brocade HBAs. You can open HCM Agent directly from the application. For more information about HCM Agent, refer to the *Brocade HCM Agent Administrator's Guide*. For more information about Brocade HBAs, refer to the documentation for the specific device.

To launch a device's Element Manager, complete the following steps.

---

**NOTE**

You must have Device Administration privileges for the selected device to launch HCM Agent. If you do not have Device Administration privileges, you will need to enter those credentials to launch HCM Agent.

---

On the Connectivity Map, double-click the Brocade HBA or CNA device you want to manage.

HCM Agent displays.

OR

On the Connectivity Map, right-click the Brocade HBA or CNA device you want to manage and select **Element Manager > Hardware**.

HCM Agent displays.

OR

1. Select a Brocade HBA or CNA.
2. Select **Configure > Element Manager > Hardware**.

HCM Agent displays.

OR

1. Select a Brocade HBA or CNA device.
2. Click the Element Manager icon on the toolbar.

HCM Agent displays.

# Adding a tool

You can specify third-party tools so they appear on the **Setup Tools** dialog box. From there, you can add them to the **Tools** menu and then open the tools directly from the Management application.

To add a tool, complete the following steps.

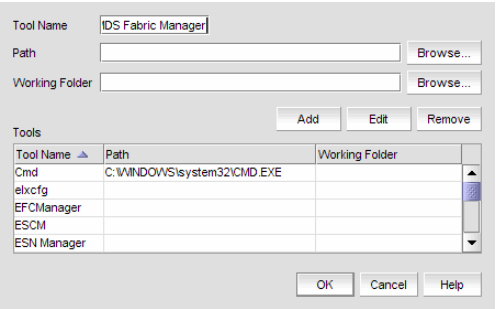
- 1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

- 2. Click the **Tools Menu** tab.

- 3. Click **Define**.

The **Define Tools** dialog box displays (Figure 64).



**FIGURE 64** Define Tools dialog box

- 4. Type the tool's name in the **Tool Name** field as you want it to appear on the **Tools** menu.
- 5. Type or browse to the path of the executable file in the **Path** field.
- 6. Type or browse to the path of the folder that you want to set as your working folder in the **Working Folder** field.
- 7. Click **Add** to add the tool.

The **Setup Tools** dialog box displays with the new tool added to the **Tools Menu Item** table.

**NOTE**

You must click **Add** before clicking **OK**; otherwise, your changes will be lost.

- 8. Click **OK** to save your work and close the **Define Tools** dialog box.
- 9. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Entering the server IP address of a tool

If the third-party tool is a web-based application, you must enter the IP address of the applications server as a parameter to be able to open the application.

To enter the server IP address, complete the following steps.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

The **Tool Menu Items** table displays all configured tools, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts.

3. Select the tool you want to edit in the **Tool Menu Items** table.

The settings for the selected tool display in the fields at the top of the dialog box.

4. Edit the IP address of the server (for example, `http://IP_Address` or `http://IP_Address:Port_Number`) in the **Parameters** field.

5. Click **Edit**.

---

**NOTE**

You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

---

6. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Adding an option to the Tools menu

You can add third-party tools to the **Tools** menu which enables you to launch tools directly from the application.

To add a option to the tools menu, complete the following steps.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

The **Tool Menu Items** table displays all configured tools, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts ([Figure 65](#)).

6 Adding an option to the Tools menu

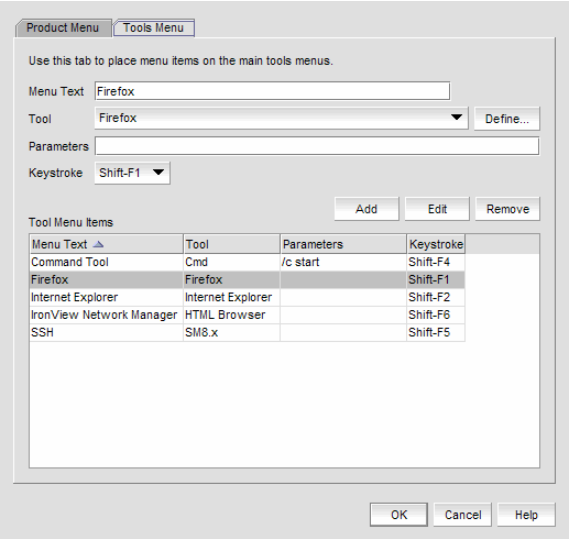


FIGURE 65 Setup Tools dialog box (Tools menu tab)

- 3. Type a label for the option as you want it to appear on the **Tools** menu in the **Menu Text** field.
- 4. Select the application from the **Tool** list, or click **Define** if you want to specify a new tool.  
To specify a new tool, refer to [“Adding a tool”](#) on page 146.
- 5. (Optional) Enter parameters, such as a URL, in the **Parameters** field.
- 6. (Optional) Select a keyboard shortcut in the **Keystroke** list.

**NOTE**  
You cannot assign the same keyboard shortcut to two different tools.

- 7. Click **Add**.  
The new tool displays in the **Tool Menu Items** table.

**NOTE**  
You must click **Add** before clicking **OK**; otherwise, the new menu option is not created.

- 8. Click **OK** to save your work and close the **Setup Tools** dialog box.  
The tool you configured now displays on the **Tools** menu.

## Changing an option on the Tools menu

You can edit parameters for third-party tools that display on the **Tools** menu.

To edit a option to the tools menu, complete the following steps.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

The **Tool Menu Items** table displays all configured tools, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts.

3. Select the tool you want to edit in the **Tool Menu Items** table.

The settings for the selected tool display in the fields at the top of the dialog box.

4. Edit the label for the option as you want it to appear on the **Tools** menu in the **Menu Text** field.
5. Select the application from the **Tool** list.
6. Edit the parameters, such as a URL, in the **Parameters** field.
7. Select a new keyboard shortcut in the **Keystroke** list.
8. Click **Edit**.

---

**NOTE**

You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

---

9. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Removing an option from the Tools menu

You can remove a tool from the third-party tool list.

To remove a option to the tools menu, complete the following steps.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

3. Select the row of the tool you want to remove in the **Tools Menu Items** table.

4. Click **Remove**.

If the tool is not being utilized, no confirmation message displays.

5. Click **Update** to remove the tool.
6. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Adding an option to a device's shortcut menu

You can add an option to a device's shortcut menu.

To add an option to the device's shortcut menu, complete the following steps.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

Click the **Product Menu** tab (Figure 66).

**FIGURE 66** Setup Tools dialog box (Product Menu tab)

The **Product Popup Menu Items** table displays all configured shortcut menu options.

2. Type or select the text in the **Menu Text** list as you want it to appear on the menu.
3. Choose one of the following options:
  - To display the menu option only for devices that meet the conditions listed, select the **Match Conditions** option.
  - To display the menu option on the shortcut menus for all devices, select the **All** option.

If you select **All**, skip to [step 7](#). Otherwise, continue to [step 4](#).
4. Select the appropriate type in the **Condition 1 Property** name list.
5. Enter the appropriate value for the selected property in the **Condition 1 Value** field.
6. (Optional) Select the **Condition 2 Property** type and enter the **Value** for that property type (Condition 1 AND Condition 2 must be true) to define a second condition to be simultaneously true.

### NOTE

To set up a condition where Condition 1 OR Condition 2 must be true, define two menu items, one for each condition.

7. Select the tool that you want to launch from the **Tool** list, or click **Define** to add a tool.  
To specify a new tool, refer to [“Adding a tool”](#) on page 146.
8. Select the **Append device ID** check box to specify the parameter used when opening the tool.
  - To specify that the device's IP address should be used when opening the tool, select the **IP Address** option.
  - To specify that the device's Node WWN should be used when opening the tool, select the **Node WWN** option.
9. Click **Add** to add the new menu item.  
It displays in the **Product Popup Menu Items** table.

**NOTE**

You must click **Add** before clicking **OK**; otherwise, your changes will be lost.

10. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Changing an option on a device's shortcut menu

You can change the parameters for a tool that displays on a device's shortcut menu.

To edit an option to the device's shortcut menu, complete the following steps.

1. Select **Tools > Setup**.  
The **Setup Tools** dialog box displays.
2. Click the **Product Menu** tab.  
The **Product Popup Menu Items** table displays all configured shortcut menu options.
3. Select the menu item you want to change in the **Product Popup Menu Items** table.  
The settings for the selected menu item display in the fields at the top of the dialog box.
4. Edit or select the text in the **Menu Text** list as you want it to appear on the menu.
5. Choose one of the following options:
  - To display the menu option only for devices that meet the conditions listed, select the **Match Conditions** option.
  - To display the menu option on the shortcut menus for all devices, select the **All** option.  
If you select **All**, skip to [step 7](#). Otherwise, continue to [step 4](#).
6. Change the type in the **Condition 1 Property** name list.
7. Change the value for the selected property in the **Condition 1 Value** field.
8. (Optional) Change the **Condition 2 Property** type or edit the **Value** for that property type (Condition 1 AND Condition 2 must be true) to edit a second condition to be simultaneously true.

**NOTE**

To set up a condition where Condition 1 OR Condition 2 must be true, define two menu items, one for each condition.

## 6 Removing an option from a device's shortcut menu

9. Select the tool from the **Tool** list that you want to launch, or click **Define** to add a tool.  
To specify a new tool, refer to [“Adding a tool”](#) on page 146.
10. Select the **Append device ID** check box to specify the parameter used when opening the tool.
  - To specify that the device's IP address should be used when opening the tool, select the **IP Address** option.
  - To specify that the device's Node WWN should be used when opening the tool, select the **Node WWN** option.
11. Click **Edit**.

---

**NOTE**

You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

---

12. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Removing an option from a device's shortcut menu

You can remove a tool that displays on a device's shortcut menu.

To remove an option to the device's shortcut menu, complete the following steps.

1. Select **Tools > Setup**.  
The **Setup Tools** dialog box displays.
2. Click the **Product Menu** tab.  
The **Product Popup Menu Items** table displays all configured menu options.
3. Select the menu item you want to remove in the **Product Popup Menu Items** table.
4. Click **Remove**.
5. Click **OK** to save your work and close the **Setup Tools** dialog box.

## VMware vCenter plug-in

---

**NOTE**

You must have host management privileges to access the **Plug-in for VMware vCenter** dialog box.

---

The VMware vCenter plug-in is a web application hosted on the Management server. This web application sends dynamic HTML content to the vSphere or VI client and the client renders the HTML content. The content includes the following:

- SAN connectivity information of each virtual machine (VM) (across all managed ESX hosts of the vCenter server)
- Switch or AG port statistics of the switch to which the Host is directly connected
- End-to-end (EE) monitor statistics (collected by EE monitors on the switch)
- SAN events based on Fabric OS events displayed in the vSphere client. These events include a crossed threshold at the switch or AG ports for transmit or receive percent utilization as well as an adapter port logging out of the fabric.

The VMware vCenter plug-in is supported on the following configurations:

- ESX 4.0 and 3.5
- vCenter 4.0
- Management application Professional Plus or Enterprise edition 10.4
- Plug-in will support managing ESX hosts with adapters from following vendors:
  - Brocade Communications
  - Q-Logic
  - Emulex

### Registering a vCenter server

1. Select **Tools > Plug-in for VMware vCenter**.

The **Plug-in for VMware vCenter** dialog box displays.

2. Click **Add**.

The **Add vCenter Server** dialog box displays.

3. Enter an IP address or fully qualified domain name for the vCenter host in the **Host** field.

The Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the operating system has IPv4 mode only or dual stack mode. The IPv6 format is valid when the operating system has IPv6 mode only or dual stack mode.

4. Enter the port number in the **Port** field.

Default is 443. Valid port number are between 1 and 65535.

5. Enter your user ID and password.

6. Click **OK** on the **Add vCenter Server** dialog box.

7. Click **Close** on the **Plug-in for VMware vCenter** dialog box.

### Editing a vCenter server

1. Select **Tools > Plug-in for VMware vCenter**.  
The **Plug-in for VMware vCenter** dialog box displays.
2. Click **Edit**.  
The **Edit vCenter Server** dialog box displays. The **Host** field is not editable in the **Edit vCenter Server** dialog box.
3. Change the port number in the **Port** field.  
Default is 443. Valid port number are between 1 and 65535.
4. Change your user ID and password.
5. Click **OK** on the **Edit vCenter Server** dialog box.
6. Click **Close** on the **Plug-in for VMware vCenter** dialog box.

### Deleting a vCenter server

1. Select **Tools > Plug-in for VMware vCenter**.  
The **Plug-in for VMware vCenter** dialog box displays.
2. Select the vCenter server you want to delete in the vCenter Servers table.
3. Click **Remove**.

# Server Management Console

---

## In this chapter

• Server management console overview .....	155
• Services .....	156
• Changing server port numbers.....	158
• Authentication .....	159
• Restoring the database.....	165
• Capturing technical support information.....	167
• Upgrading HCM on the Management server.....	168
• SMI Agent configuration .....	169

## Server management console overview

The Server Management Console (SMC) is an automatically installed, stand-alone application for managing the Management application server. You can perform the following tasks using the SMC:

- From the **Services** tab, you can start, stop, refresh, and restart services on the server.
- From the **Ports** tab, you can change the Management application server or web server port number.
- From the **Authentication** tab, you can configure an authentication server (LDAP or Radius server), and establish authentication policies.
- From the **Restore** tab, you can restore server application data.
- From the **Technical Support Information** tab, you can collect information for technical support.
- From the **HCM Upgrade** tab, you can upgrade the Management application to use a new version of Host Connectivity Manager (HCM).
- From the **SMI Agent Configuration Tool** dialog box, you can configure the SMI Agent settings, such as security, CIMOM, and certificate management as well as launch Management application dialog boxes.

## Launching the SMC on Windows

Open the **Server Management Console** from the **Start** menu on the Management application server.

You can also drag the SMC icon onto your desktop as a short cut.

## Launching the SMC on Linux and Solaris

Perform the following steps to launch the server management console on Linux and Solaris systems.

1. On the Management application server, go to the following directory:

*Install\_Directory/bin*

2. Type the following at the command line:

```
. /smc
OR
sh smc
```

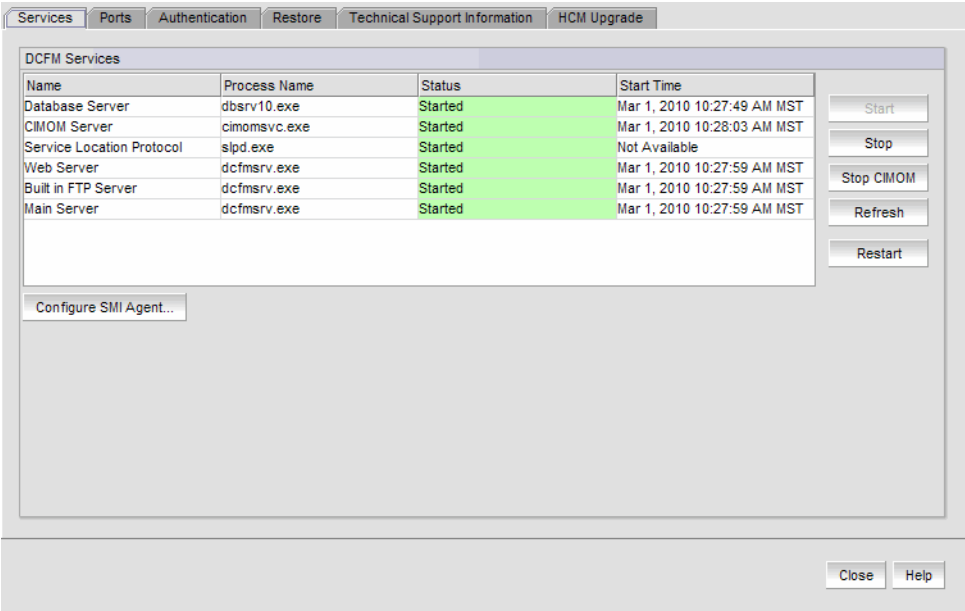
## Services

You must be logged in at the administrator (Windows systems) or root (UNIX systems) level to stop, start, and restart the Management application services. Stopping and restarting the Management application services causes clients connected to the server to lose connection, and they must re-log in to the server.

## Monitoring and managing Management application services

To monitor the status of the Management application services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab ([Figure 67](#)).



**FIGURE 67** Services tab

3. Review the following information for each available service.
  - **Name**—The name of the server; for example, FTP Server or Database Server.
  - **Process Name**—The name of the process; for example, dbsrv10.exe (Database Server).
  - **Status**—The status of the service; for example, started or stopped.
  - **Start Time**—The date and time the service started. The Start Time for Service Location Protocol displays as 'Not Available'.
4. Click **Close** to close the Server Management Console.

## Refreshing the server status

To refresh the server status for each of the Management application services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Refresh** to update the table with the latest status of the services in case the services were stopped or restarted outside of the Server Management Console.
4. Click **Close** to close the Server Management Console.

## Stopping all services

To stop all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Stop** to stop all services.

Note that clicking **Restart** stops and then restarts all services.
4. Click **Close** to close the Server Management Console.

## Stopping the CIMOM services

To stop the CIMOM (Common Information Model Object Manager) services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Stop CIMOM**.
4. Click **Close** to close the Server Management Console.

## Starting all services

---

**NOTE**

The **Start** button restarts running services in addition to starting stopped services which causes client-server disconnect.

---

To start all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Start** to start all services.

---

**NOTE**

If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.

---

4. Click **Close** to close the Server Management Console.

## Restarting all services

To stop and restart all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Restart** to stop then restart all services.

---

**NOTE**

If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.

---

4. Click **Close** to close the Server Management Console.

## Changing server port numbers

Use the **Ports** tab of the Server Management Console to change the Management application server and Web server port numbers. The default Web Server port number is 80. The Management application server default port number is 24600.

To change the Management application server or web server port number, complete the following steps.

1. Click the **Ports** tab.
2. Type a new port number in the *Management\_Application\_Name* **Server** or **Web Server port** field.

Do not use port 2638.

3. Click **Apply** to save the changes.

The server automatically restarts if you change the server port number. You must manually restart the server if you change only the web server port number.

# Authentication

The Authentication function enables you to configure an authentication server and establish authentication policies. Authentication is configured to the local database by default. If you configure primary authentication to a Radius server, an LDAP server, or switch authentication, you can also configure secondary authentication to the local server. When you log in to the Management application, if the primary server is unavailable, the Management application attempts with the next configured primary server. If all primary servers are unavailable, then the Management application falls back to the secondary authentication. Fall back only occurs for server unavailability, not if there is an authentication failure for another reason (for example, invalid credentials).

## Configuring a Radius server

If you are using a Radius server for authentication, make the following preparations first:

- Select an **Authentication Type** (you will be prompted to provide a type in the **Add or Edit Radius Server** dialog box). The **Authentication Type** is the authentication policy you choose for handling authentication. The options are PAP and CHAP.
  - PAP, password protected protocol, is based on password verification. Passwords are not encrypted, and are not secure from eavesdroppers during transmission.
  - CHAP, challenge handshake protocol, uses a three-way handshake method of verification based on a shared secret. If you are using CHAP, have the shared secret available to you. You will need to type it in as a configuration parameter.
- Know the Shared Secret.
- Have the IP address of the server available.
- Know the TCP port you are using. For Radius servers, ports 1812 or 1645 (actually UDP ports) are commonly used. Check with the Radius server vendor if you are not sure which port to specify.
- Know how long you want to wait between attempts to reach the server if it is busy. This is expressed as a timeout value (default is 3 seconds) in seconds. Values are between 1 and 15.
- Determine how many attempts (default is 3 times) to make to reach the server before stopping and assuming it is unreachable. Values are between 1 and 5.
- If possible, establish an active connection with the Radius server before configuration. This enables you to test the connection as part of the configuration procedure.

## 7 Configuring a Radius server

1. Select the **Authentication** tab (Figure 68).

The screenshot shows the 'Authentication' tab of a configuration window. At the top, there are tabs for 'Services', 'Ports', 'Authentication', 'Restore', 'Technical Support Information', and 'HCM Upgrade'. Below the tabs, a message states: 'This DCFM server currently uses Radius Server as the primary authentication, and Local Database as the secondary Authentication.' Below this message, there are two dropdown menus: 'Primary Authentication' set to 'Radius Server' and 'Secondary Authentication' set to 'Local Database'. A table titled 'Radius Servers and Sequence' is displayed, with columns: 'IP Address', 'TCP Port', 'Timeout(Sec)', 'Attempts', and 'Authentication Type'. The table is currently empty. To the right of the table are 'Move Up' and 'Move Down' buttons. Below the table are 'Add', 'Edit', and 'Remove' buttons. At the bottom left, there is an 'Authentication Audit Trail' section with a 'Display' button. At the bottom right, there are 'Test' and 'Apply' buttons. At the very bottom, there are 'Close' and 'Help' buttons.

**FIGURE 68** Authentication tab

2. For **Primary Authentication**, select **Radius Server**.
3. Click **Add**.

The **Add or Edit Radius Server** dialog box displays (Figure 69).

The screenshot shows the 'Add or Edit Radius Server' dialog box. It contains several input fields: 'IP Address' (a text box), 'TCP Port' (a text box), 'Authentication Type' (a dropdown menu currently set to 'CHAP'), 'Shared Secret' (a text box), 'Confirm Secret' (a text box), 'Timeout(Sec)' (a text box), and 'Attempts' (a text box). At the bottom right, there are 'Ok' and 'Cancel' buttons.

**FIGURE 69** Add or Edit Radius Server

4. Enter the radius server's IP address in the **IP Address** field.
5. Enter the TCP port used by the Radius server in the **TCP Port** field.
6. Select the authentication policy (PAP or CHAP) from the **Authentication Type** field.
7. Enter the shared secret in the **Shared Secret** and **Confirm Secret** fields.
8. Enter the timeout timer value (in seconds) that specifies the amount of time to wait between retries when the server is busy in the **Timeout (Sec)** field.
9. Enter the number of attempts to be made to reach a server before assuming it is unreachable in the **Attempts** field.

10. Click **OK** to return to the **Authentication** tab.
11. If you have established an active connection with the Radius server, click **Test**.  
Test attempts to contact the Radius server by issuing a **ping** command.
12. Click **Apply** to save the configuration.

## Configuring an LDAP server

If you are using an LDAP server for authentication, make the following preparations first:

- Have the IP address of the server available.
- Know the TCP port you are using. The LDAP server uses Transport Layer Security (TLS). LDAP over TLS generally uses port 389. Check with the LDAP server administrator if you are not sure which port to specify.
- Know how long you want to wait between attempts (default is 3 seconds) to reach the server if it is busy. This is expressed as a timeout value in seconds. Values are between 1 and 15.
- Determine how many attempts (default is 3 times) to make to reach the server before stopping and assuming it is unreachable. Values are between 1 and 5.

To configure an LDAP server for authentication, complete the following steps.

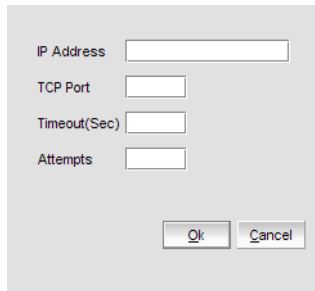
1. Select the **Authentication** tab.
2. Select **LDAP Server** from the **Primary Authentication** list.

The screenshot shows the 'Authentication' tab of a configuration window. At the top, there are tabs: Services, Ports, Authentication (selected), Restore, Technical Support Information, and HCM Upgrade. Below the tabs, a message states: 'This DCFM server currently uses LDAP Server as the primary authentication, and Local Database as the secondary Authentication.' Below this message are two dropdown menus: 'Primary Authentication' set to 'LDAP Server' and 'Secondary Authentication' set to 'Local Database'. Below these is a label 'Switch to secondary authentication when' followed by a dropdown menu set to 'LDAP Servers are not reachable'. The main section is titled 'LDAP Servers and Sequence' and contains a table with columns: IP Address, TCP Port, TimeOut(Sec), and Attempts. The table is currently empty. To the right of the table are 'Move Up' and 'Move Down' buttons. Below the table are 'Add', 'Edit', and 'Remove' buttons. At the bottom left is 'Authentication Audit Trail' with a 'Display' button. At the bottom right are 'Test' and 'Apply' buttons. At the very bottom are 'Close' and 'Help' buttons.

**FIGURE 70** Authentication tab - LDAP server

3. Click **Add**.

The **Add or Edit LDAP Server** dialog box displays (Figure 71).



**FIGURE 71** Add or Edit LDAP server

4. Enter the LDAP server's IP address in the **IP Address** field.
5. Enter the TCP port used by the Radius server in the **TCP Port** field.
6. Enter the timeout timer value (in seconds) that specifies the amount of time to wait between retries when the server is busy in the **Timeout (Sec)** field.
7. Enter the number of attempts to be made to reach a server before assuming it is unreachable in the **Attempts** field.
8. Click **OK** to return to the **Authentication** tab.
9. If you have established an active connection with the LDAP server, click **Test**.  
Test attempts to contact the LDAP server by issuing a **ping** command.
10. Set secondary authentication by selecting **Local Database** from the **Secondary Authentication** list.
11. Set the fall back condition to secondary authentication by selecting one of the following options from the **Switch to secondary authentication when** list:
  - **LDAP servers are not reachable**
  - **User not found in LDAP**
12. Click **Apply** to save the configuration.

## Configuring switch authentication

Switch authentication enables you to authenticate a user account against the switch database and the Management application server. You can configure up to three switches and specify the fall back order if one or more of the switches is not available.

---

### NOTE

Switch authentication is only supported on Fabric OS devices.

---

To configure switch authentication, complete the following steps.

1. Select the **Authentication** tab.
2. For **Primary Authentication**, select **Switch**.

3. Enter the switch IP address and click **Add**.  
Repeat step 3 as needed. You can add up to three switches.
4. Set up the fall back order by completing the following steps.
  - a. Select the IP address of the switch you want to move.
  - b. Click **Move Up** or **Move Down** to move the switch where you want it.
5. Select a switch and click **Remove** to remove a switch from the list.
6. Click **Test**.  
The **Test Authentication** dialog box displays.
7. Enter your user ID and password and click **Test**.  
Test verifies your user ID and password on the switch and verifies user privileges on the Management application server.
8. Click **Apply** to save the configuration.

## Configuring Windows authentication

Windows authentication enables you to authenticate a user account against the Windows user accounts and the Management application server when running on Windows hosts.

The following list details the supported Windows authentication types and the associated platforms:

- NT domain authentication (multiple domains)—supported on Windows XP/2003/2008 platforms only
- Windows Workgroup authentication—supported on Windows XP/2003/2008 platforms only
- Windows local user accounts—supported on Windows XP/2003/2008 platforms only.

To configure Windows authentication, complete the following steps.

1. Select the **Authentication** tab.
2. For **Primary Authentication**, select **Windows Domain**.
3. Enter the domain name in the **Windows Domain Name** field.
4. Click **Test**.  
The **Test Authentication** dialog box displays.
5. Enter your user ID and password and click **Test**.  
Test verifies your user ID and password on the Windows domain and verifies user privileges on the Management application server.
6. Click **Apply** to save the configuration.

## Configuring NIS authentication

Network Information Services (NIS/NIS+) authentication enables you to authenticate a user account against the NIS user account and the Management application server when running on UNIX platforms.

To configure NIS authentication, complete the following steps.

1. Select the **Authentication** tab.
2. For **Primary Authentication**, select **NIS**.
3. Enter the NIS IP address in the **NIS Host Name/ IP Address** field.
4. Enter the NIS domain name in the **NIS Domain Name** field.
5. Click **Test**.

The **Test Authentication** dialog box displays.

6. Enter your user ID and password and click **Test**.

Test verifies your user ID and password for NIS authentication and verifies user privileges on the Management application server.

7. Click **Apply** to save the configuration.

## Configuring UNIX password file authentication

UNIX password file (etc/password) authentication enables you to authenticate a user account against the UNIX user account and the Management application server when running on UNIX platforms.

To configure UNIX password file authentication, complete the following steps.

1. Select the **Authentication** tab.
2. For **Primary Authentication**, select **Password File**.
3. Click **Test**.

The **Test Authentication** dialog box displays.

4. Enter your user ID and password and click **Test**.

Test verifies your user ID and password for UNIX password file authentication and verifies user privileges on the Management application server.

5. Click **Apply** to save the configuration.

## Configuring local database authentication

Local database authentication enables you to authenticate a user account against the local database and the Management application server.

To configure local database authentication, complete the following steps.

1. Select the **Authentication** tab.
2. For **Primary Authentication**, select **Local Database**.

3. Click **Test**.

The **Test Authentication** dialog box displays.

4. Enter your user ID and password and click **Test**.

Test verifies your user ID and password for the local database and verifies user privileges on the Management application server.

5. Click **Apply** to save the configuration.

## Displaying the client authentication audit trail

All responses to authentication requests coming from clients are logged to an audit trail log file. This file is automatically backed up on the first day of every month.

1. Select the **Authentication** tab.

2. Click **Display** next to **Authentication Audit Trail**.

The **Login** dialog box displays.

3. Enter your username and password in the appropriate fields and click **OK**.

The defaults are Administrator and password, respectively.

The **Authentication Audit Trail** log displays.

The audit trail shows user names that have attempted to log in to the Management application, and changes to user authentication.

4. Click the **Client to Server Authentication** tab to view the client to server authentication status.
5. Click the **Authentication Settings Changes** tab to view the previous authentication changes.

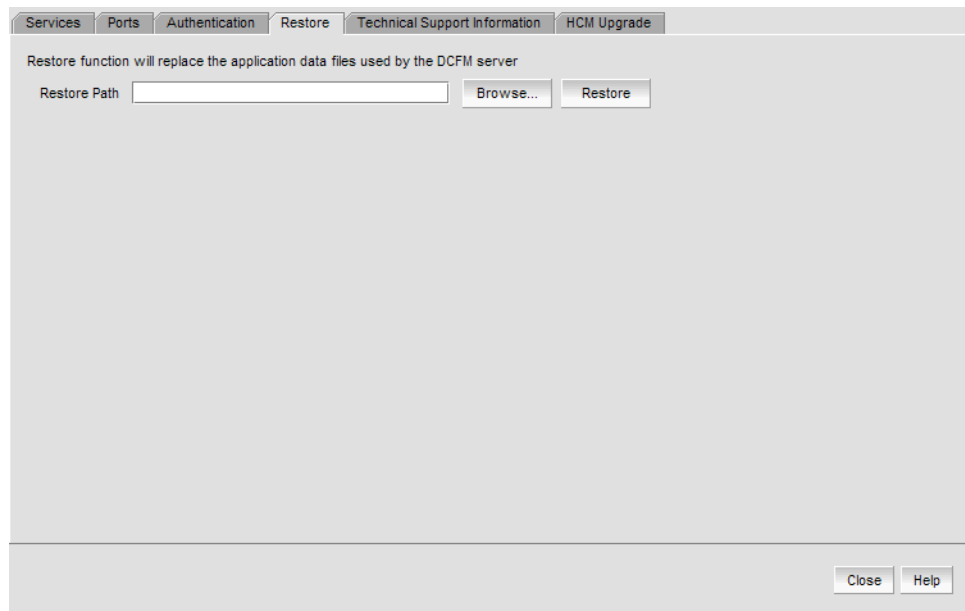
## Restoring the database

To restore application data files, you must know the path to the backup files. This path is configured from the **Server > Options** dialog box. For more information about backup, refer to [“Data backup”](#) on page 59.

To restore the application data files, complete the following steps.

1. Click the **Services** tab.
2. Stop all services.
3. Click the **Restore** tab ([Figure 72](#)).

## 7 Restoring the database



**FIGURE 72** Restore tab

4. Click **Browse** to select the path (defined in the **Output Directory** field on the **Options** dialog box - **Backup** pane) to the database backup location.
5. Click **Restore**.

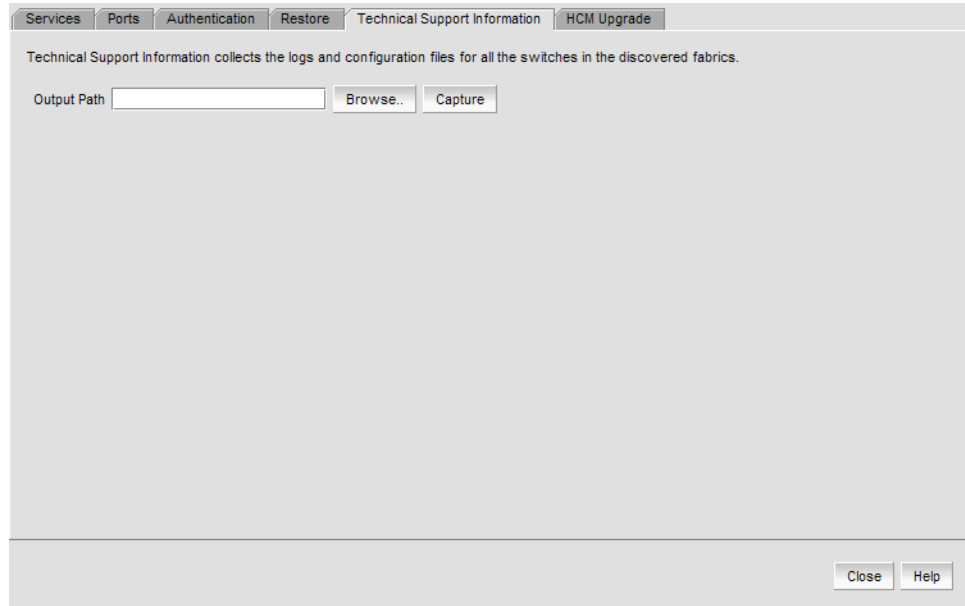
Upon completion, a message displays the status of the restore operation. Click **OK** to close the message and the Server Management Console. For the restored data to take effect, re-launch the Configuration Wizard using the instructions in [“Launching the Configuration Wizard”](#) on page 18.

## Capturing technical support information

The **Technical Support Information** tab of the SMC allows you to capture technical support information for the Management application as well as the configuration files for all switches in discovered fabrics. This information is saved in a *zip* file in a location that you specify.

To capture technical support information, complete the following steps.

1. Select the **Technical Support Information** tab (Figure 73).



**FIGURE 73** Technical Support Information tab

2. Click **Browse** to select the path where the **supportShow** data will be saved.

If you do not specify an output path, the Management application automatically saves the data to the *Install\_Home/support* directory.

---

**NOTE**

For Linux systems, you cannot have blank spaces in the output path (target directory). If the output path contains blank spaces, the supportShow files are not complete.

---

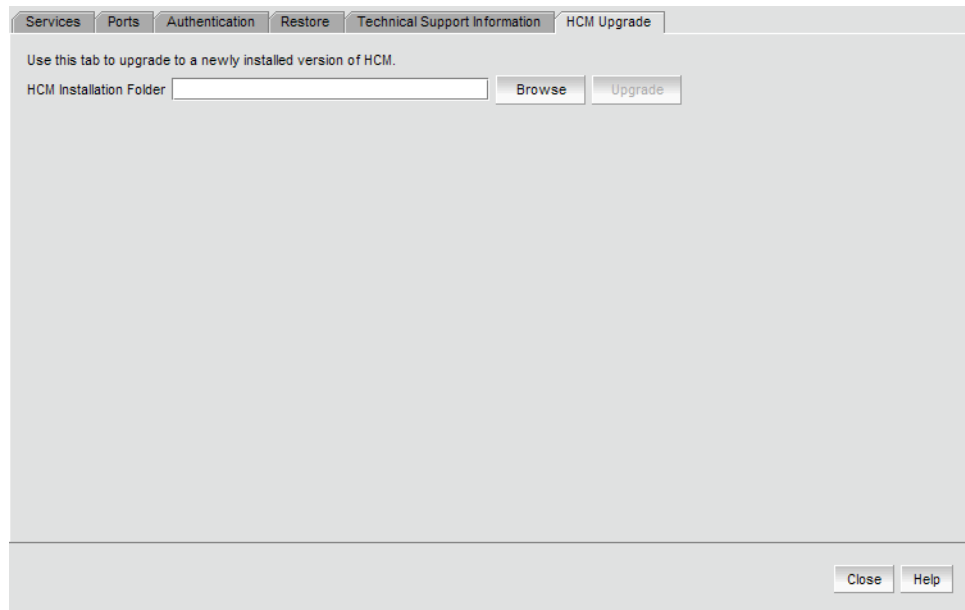
3. Click **Capture**.  
A confirmation message displays when the capture is complete.
4. Click **OK**.

## Upgrading HCM on the Management server

The **HCM Upgrade** tab enables you to upgrade the Management application to include a new version of HCM.

To upgrade HCM, complete the following steps.

1. Select the **HCM Upgrade** tab ([Figure 74](#)).



**FIGURE 74** HCM Upgrade tab

2. Click **Browse** to select the HCM installation folder location (for example, C:\Program Files\BROCADE\Adapter on Windows systems and /opt/brocade/adapter on Solaris and Linux systems).
3. Click **Upgrade**.
4. Click **Close**.

## SMI Agent configuration

The SMIA Configuration Tool enables you to configure SMI Agent settings, such as security, CIMOM, and certificate management. This tool is automatically installed with the Management application as part of the Server Management Console. This SMIA Configuration Tool consists of the following tabs:

- **Home**—enables you to launch the following Management application dialog boxes: **Discovery**, **Users**, **Options**, **Server**, and **About**.
- **Authentication**—enables you to configure mutual authentication for Client and Indication using a secure protocol.
- **CIMOM**—enables you to configure the CIMOM server port, the Bind Network Address, and the CIMOM log.
- **Certificate Management**—enables you to import Client and Indication certificates, export Server certificates, as well as view and delete current certificates.
- **Summary**—enables you to view the CIMOM server configuration and current configuration.

### Launching the SMIA configuration tool on Windows

#### NOTE

All Management application services must be running before you can log into the **SMIA Configuration Tool**. To start the Management application services, click **Start** on the **Server Management Console** dialog box.

1. Launch the **Server Management Console** from the **Start** menu on the Management application server.

You can also drag the SMC icon onto your desktop as a short cut.

2. Click **Configure SMI Agent** on the **Server Management Console** dialog box.

The **Log In** dialog box displays ([Figure 75](#)).

The image shows a 'Log In' dialog box with the title 'Enter User ID and Password to log onto the server'. It contains the following fields and controls:

- Network Address:** A text field containing 'localhost'.
- Server Name:** A text field containing '6b3s0f1'.
- User ID:** A text field containing 'Administrator'.
- Password:** A text field with masked characters (dots).
- Save password:** A checked checkbox.
- Login/Exit buttons:** Two buttons at the bottom right labeled 'Login' and 'Exit'.
- Status:** A small icon and text 'Server Available' at the bottom left.

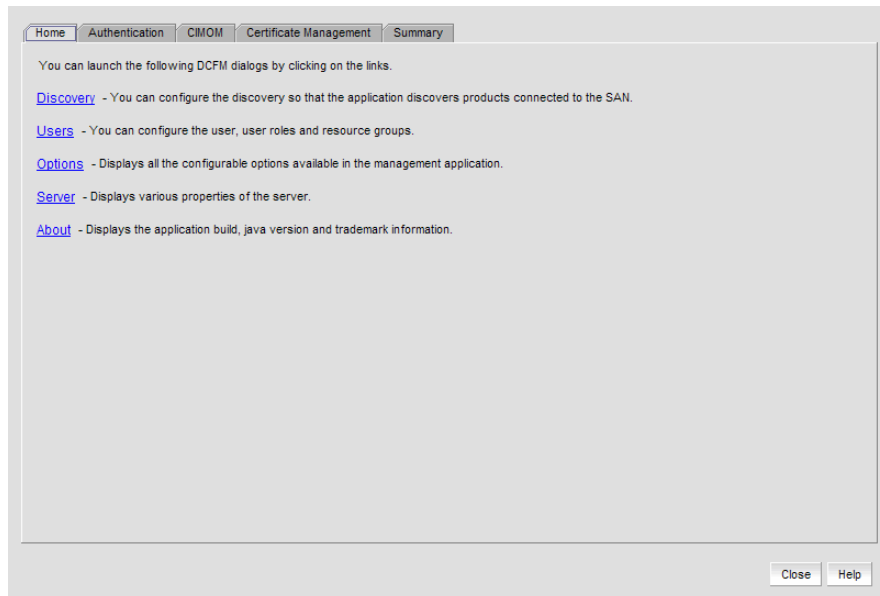
**FIGURE 75** Log In dialog box

3. Enter your username and password in the appropriate fields.

The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
5. Click **Login**.

The **SMIA Configuration Tool** dialog box displays (Figure 76).



**FIGURE 76** SMIA Configuration Tool dialog box

## Launching the SMIA configuration tool on Linux and Solaris

### NOTE

All Management application services must be running before you can log into the **SMIA Configuration Tool**. To start the Management application services, click **Start** on the **Server Management Console** dialog box.

Perform the following steps to launch the server management console on Linux and Solaris systems.

1. On the Management application server, go to the following directory:

*Install\_Directory/bin*

2. Type the following at the command line:

```
./smc
OR
sh smc
```

3. Click **Configure SMI Agent** on the Server Management Console dialog box.

The **Login** dialog box displays.

4. Enter your username and password in the appropriate fields and click **OK**.

The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

The **SMIA Configuration Tool** dialog box displays.

## Launching a remote SMIA configuration tool

To launch a remote SMIA configuration tool, complete the following steps.

1. Open a web browser and enter the IP address of the Management application server in the **Address** bar.

If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP\_Address:Web\_Server\_Port\_Number*.

The Management application web start screen displays.

2. Click the SMIA configuration tool application web start link.

The **Log In** dialog box displays.

3. Enter your user name and password.

The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

5. Click **Login**.

The **SMIA Configuration Tool** dialog box displays

## Home tab

The **Home** tab of the **SMIA Configuration Tool** enables you to access the following Management application features or information:

- **Discovery**—enables you to view discovered fabrics, discover new fabrics, as well as edit the default SNMP configuration. For step-by-step instructions, refer to [“Fabric discovery overview”](#) on page 35.
- **Users**—enables you to create or delete Management application users with System Administrator privileges. For step-by-step instructions, refer to [“Users”](#) on page 351.
- **Options**—enables you to configure the Management application settings. For step-by-step instructions, refer to [Chapter 3, “Application Configuration”](#).
- **Server**—enables you to view server properties. For step-by-step instructions, refer to [“Viewing server properties”](#) on page 24.
- **About**—enables you to display information about the Management application, including the build number, Java version, and trademark information.

### *Accessing Management application features*

To access Management application features such as, discovery, role-based access control, application configuration and display options, server properties, as well as the application name, build, and copyright, complete the following steps.

1. Click the **Home** tab, if necessary.
2. Select from the following to access the feature or dialog box.
  - **Discovery**
  - **Users**
  - **Options**
  - **Server**
  - **About**
3. Click **Close** to close the **SMIA Configuration Tool** dialog box.

### **Authentication**

The **Authentication** tab enables you to configure mutual authentication for Client and Indication using a secure protocol.

### *Enabling or disabling CIM client and indication mutual authentication*

When you enable client mutual authentication, all CIM client and indication requests to the SMI Agent must pass credentials (KeyStore and TrustStore) to validate the requests. The KeyStore file provides the credentials and the TrustStore file verifies the credentials. When you enable indication mutual authentication, both the CIM client and the CIMOM server maintain the TrustStore files.

The CIM client KeyStore file sends credentials to be validated by the CIMOM server TrustStore file for any communication from the CIM client to the CIMOM server and the CIMOM server KeyStore file sends credentials to be validated by the CIM client TrustStore file for any communication from the CIMOM server to the CIM client

To enable or disable CIM client and indication mutual authentication, complete the following steps.

1. Click the **Authentication** tab.

The screenshot shows the 'Authentication' tab of a configuration window. At the top, there are tabs for 'Home', 'Authentication', 'CIMOM', 'Certificate Management', and 'Summary'. The 'Authentication' tab is active. Below the tabs, there are two unchecked checkboxes: 'Enable Client Mutual Authentication' and 'Enable Indication Mutual Authentication'. Under the heading 'CIMOM Server Authentication', there are two radio buttons: 'No Authentication' (unselected) and 'DCFM Authentication' (selected). Below these, a text label reads 'Provide the DCFM Server credentials for CIMOM to communicate to the server.' There are two input fields: 'Username' with the text 'Administrator' and 'Password' with masked characters '\*\*\*\*\*'. An 'Apply' button is located below the password field. At the bottom of the main content area, a message with an information icon states: 'Changes will take effect at the next CIMOM restart. CIMOM server can be restarted from DCFM Server Management Console.' At the bottom right of the window, there are 'Close' and 'Help' buttons.

**FIGURE 77** Authentication tab

2. Select the **Enable Client Mutual Authentication** check box, as needed.  
If the check box is checked, CIM client mutual authentication is enabled. If the check box is clear (default), client mutual authentication is disabled.
3. Select the **Enable Indication Mutual Authentication** check box, as needed.  
If the check box is checked, indication mutual authentication is enabled. If the check box is clear (default), client mutual authentication is disabled.
4. Click **Apply**.

---

**NOTE**

Changes on this tab take effect after the next CIMOM server restart.

---

5. Click **Close** to close the **SMIA Configuration Tool** dialog box.

### *Configuring CIMOM server authentication*

CIMOM server authentication is the authentication mechanism between the CIM client and the CIMOM Server. You can configure the CIMOM server to allow the CIM client to query the CIMOM server without providing credentials; however, the CIMOM server requires the Management application credentials to connect to the Management application server to retrieve the required data. Therefore, if you select no authentication, you must provide Management application credentials to retrieve data from the Management application server.

To configure CIMOM server authentication, complete the following steps.

1. Click the **Authentication** tab.
2. Choose from one of the following options:
  - Select **No Authentication** to allow the CIM client to query the CIMOM server without providing credentials; however, note that the CIMOM server requires the Management application credentials to connect to the Management application server to retrieve the required data. To provide Management application credentials, complete the following steps.
    - a. Enter the Management application user name in the **Username** field.
    - b. Enter the Management application user password in the **Password** field.
  - Select **Management\_Application Authentication** to allow the CIM client to query the CIMOM server and the Management application server using the credentials configured on the **Users** tab.
3. Click **Apply**.

---

**NOTE**

Changes on this tab take effect after the next CIMOM server restart.

---

4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

## CIMOM configuration

### NOTE

You must have Security Read and Write privileges to make changes on the CIMOM tab.

The **CIMOM** tab enables you to configure the CIMOM server port, the Bind Network Address, and the CIMOM log.

### *Configuring the SMI Agent port number*

To configure the SMI Agent port number, complete the following steps.

1. Click the **CIMOM** tab.

Home Authentication **CIMOM** Certificate Management Summary

Configure HTTP and HTTPS connections between the CIMOM and CIM Client

Enable SSL ☒

SMI Agent Port#

Current Value

Default Value

IP Configuration

Bind Network Address

CIMOM Logs will be written into cimom/server/logs folder

Log Level

File Size  MB

Number of Files

Changes will take effect at the next CIMOM restart. CIMOM server can be restarted from DCFM Server Management Console.

**FIGURE 78** CIMOM tab

2. Select or clear the **Enable SSL** check box, to enable or disable SSL for the SMI Agent.

### NOTE

Disabling SSL will disable Indication and Client Mutual Authentication.

If the check box is checked (default), SSL is enabled. If the check box is clear, SSL is disabled.

3. Enter the SMI Agent port number in the **SMI Agent Port #** field.

This port number must be within the range of 1 through 65535. Defaults are 5989 with SSL enabled and 5988 with SSL disabled.

4. Click **Apply**.

---

**NOTE**

Changes on this tab take effect after the next CIMOM server restart.

---

If you disabled SSL, a confirmation message displays. Click **Yes** to continue.

5. Click **Close** to close the **SMIA Configuration Tool** dialog box.

## *Configuring the Bind Network Address*

---

**NOTE**

You must have Security Read and Write privileges to make changes on the **CIMOM** tab.

---

To configure the network bind address, complete the following steps.

1. Click the **CIMOM** tab.
2. Select a network address from the **IP Configuration Bind Network Address** list to which you want to bind the CIMOM server.

The default network address is the host system name.

3. Click **Apply**.

---

**NOTE**

Changes on this tab take effect after the next CIMOM server restart.

---

4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

## *Configuring the CIMOM log*

---

**NOTE**

You must have Security Read and Write privileges to make changes on the **CIMOM** tab.

---

To configure the CIMOM log, complete the following steps.

1. Click the **CIMOM** tab.
2. Select a log category from the **Log Level** list to start logging support data for the server.

Options include the following:

- Off—select to turn off logging support data.
- Severe—select to only log support data that indicates serious failures which prevent normal program operation.
- Warning—select to only log support data that indicates a potential problem.
- Info (default)—select to only log support data for informational messages.
- Config—select to only log support data for static configuration messages used to assist in debugging problems associated with particular configurations.
- Fine—select to only log message data used to provide trace information.

- Finer—select to only log message data used to provide detailed trace information.
- Finest—select to only log message data used to provide highly detailed trace information.
- All—select to log support data for all messages.

3. Click **Apply**.

#### NOTE

Changes on this tab take effect after the next CIMOM server restart.

4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

## Certificate management

#### NOTE

You must have Security Read and Write privileges to view or make changes on the **Certificate Management** tab.

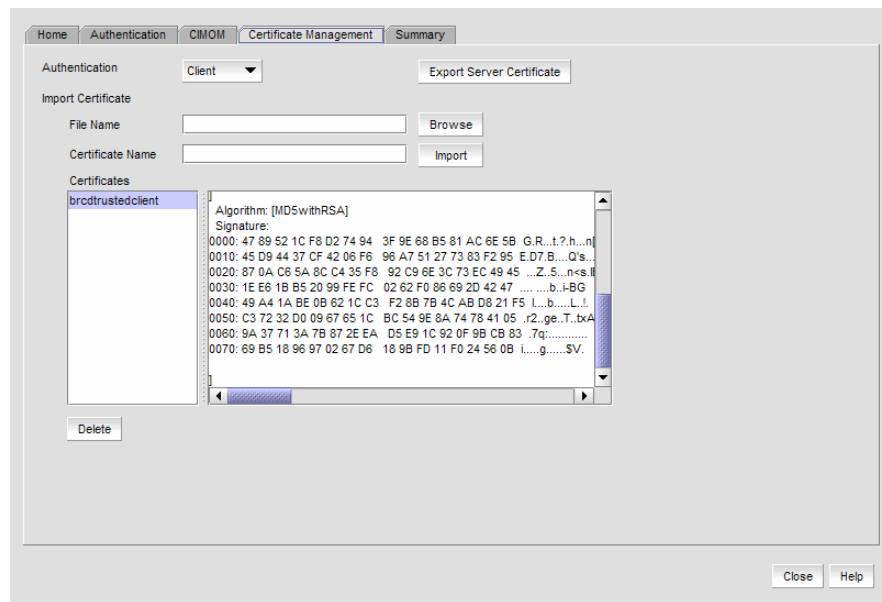
The **Certificate Management** tab enables you to manage your CIM client and Indication authentication certificates. Using this tab, you can perform the following operations:

- “Importing a certificate”
- “Viewing a certificate”
- “Exporting a certificate”
- “Deleting a certificate”

### *Importing a certificate*

To import a certificate, complete the following steps.

1. Click the **Certificate Management** tab.



**FIGURE 79** Certificate Management tab

2. Select the **Client** or **Indication** from the **Authentication** list.

The appropriate certificates display in the **Certificates** list.

3. Enter the full path or browse to the certificate you want to import (for example, C:\Certificates\cimom-indication-auth2.cer).

You can only import certificate files with the CER extension (.cer).

4. Enter a name for the certificate in the **Certificate Name** field.

5. Click **Import**.

The new certificate displays in the **Certificates** list and text box.

If the certificate location is not valid, an error message displays. Click **OK** to close the message and reenter the full path to the certificate location.

If you did not enter a certificate name, an error message displays. Click **OK** to close the message and enter a name for the certificate.

If the certificate file is empty or corrupted, an error message displays. Click **OK** to close the message.

6. Click **Close** to close the **SMIA Configuration Tool** dialog box.

### *Viewing a certificate*

---

#### **NOTE**

You must have Security Read and Write privileges to view the **Certificate Management** tab.

---

To view a certificate, complete the following steps.

1. Select **Client** or **Indication** from the **Authentication** list.

The appropriate certificates display in the **Certificates** list.

2. Select the certificate you want to view in the **Certificates** list.

The certificate details display in the **Certificates** text box.

3. Click **Close** to close the **SMIA Configuration Tool** dialog box.

### *Exporting a certificate*

---

#### **NOTE**

You must have Security Read and Write privileges to view or make changes to the **Certificate Management** tab.

---

To export a certificate, complete the following steps.

1. Click the **Certificate Management** tab.

2. Select **Client** or **Indication** from the **Authentication** list.

The appropriate certificates display in the **Certificates** list.

3. Select the certificate you want to export in the **Certificates** list.

4. Click **Export Server Certificate**.

The **Save As** dialog box displays.

5. Browse to the directory where you want to export the certificate.
6. Edit the certificate name in the **File Name** field, if necessary.
7. Click **Save**.
8. Click **Close** to close the **SMIA Configuration Tool** dialog box.

### *Deleting a certificate*

---

**NOTE**

You must have Security Read and Write privileges to view or make changes to the **Certificate Management** tab.

---

To delete a certificate, complete the following steps.

1. Click the **Certificate Management** tab.
2. Select **Client** or **Indication** from the **Authentication** list.  
The appropriate certificates display in the **Certificates** list.
3. Select the certificate you want to delete in the **Certificates** list.
4. Click **Delete**.
5. Click **Yes** on the confirmation message.  
The selected certificate is removed from the **Certificates** list.
6. Click **Close** to close the **SMIA Configuration Tool** dialog box.

## Viewing the configuration summary

To view summary information about the Server configuration and the current configuration, complete the following steps.

1. Click the **Summary** tab.

**FIGURE 80** Summary tab

2. Review the summary.

### NOTE

When the CIMOM server is stopped, the server configuration information does not display on the **Summary** tab.

The following information is included in the summary.

Field/Component	Description
<b>Client Mutual Authentication</b>	Displays whether or not the client mutual authentication is enabled or disabled for the Server Configuration and the Current Configuration.
<b>Indication Mutual Authentication</b>	Displays whether or not the indication mutual authentication is enabled or disabled for the Server Configuration and the Current Configuration.
<b>CIMOM Server Authentication</b>	Displays whether or not the CIMOM server authentication is enabled or disabled for the Server Configuration and the Current Configuration.
<b>User Name</b>	Displays the user name for the Server Configuration and the Current Configuration. Only displays if <b>CIMOM Server Authentication</b> is No Authentication.
<b>SSL</b>	Displays whether or not the SSL is enabled or disabled for the Server Configuration and the Current Configuration.
<b>SMI Agent Port #</b>	Displays the SMI Agent port number for the Server Configuration and the Current Configuration.

Field/Component	Description
Bind Network Address	Displays the Bind Network address for the Server Configuration and the Current Configuration.
Log Level	Displays the log level for the Server Configuration and the Current Configuration. Options include the following: <ul style="list-style-type: none"><li>• 10000—Off</li><li>• 1000—Severe</li><li>• 900—Warning</li><li>• 800—Info (default)</li><li>• 700—Config</li><li>• 500—Fine</li><li>• 400—Finer</li><li>• 300—Finest</li><li>• 0—All</li></ul>
Managed Ports	Displays the number of managed ports. For more information about managed port count rules, refer to <a href="#">“Managed port count calculation”</a> .
Licensed Ports	Displays the number of licensed ports.

3. Click **Close** to close the **SMIA Configuration Tool** dialog box.

## 7 Viewing the configuration summary

# Device Configuration

---

## In this chapter

• Configuration repository management .....	183
• Device properties. ....	192
• Enhanced group management .....	196
• Firmware management .....	197
• Host port mapping .....	201
• Ports .....	206
• Port Auto Disable .....	221
• Storage port mapping configuration .....	224
• Device Technical Support .....	230
• Upload Failure data capture .....	234

## Configuration repository management

Configuration files are stored in an SQL database on the Management application server. You can save entire configurations of switch configuration files and use them to ensure consistent switch settings in your fabric, propagate configuration settings to additional switches in the fabric, and troubleshoot the switches.

For Windows platforms the default location is  
Install\_Home\data\database\*Management\_Application\_Name*.db

For more information about the database fields, refer to [“Sybase and Derby Database Fields”](#) on page 719.

## Saving switch configurations

### NOTE

Save switch configuration is only supported on Fabric OS switches.

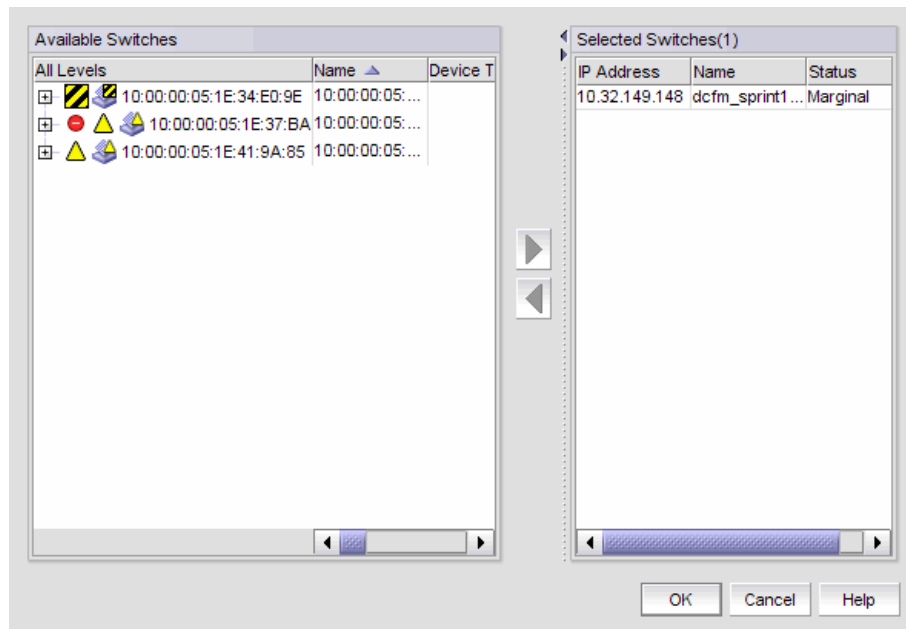
### NOTE

To save switch configuration on more than one switch at a time, you must have the Enhanced Group Management license.

Configuration files are uploaded from the selected switches and stored in individual files. Files are named with the convention *cfg\_fabricName\_switchName\_domainID*.

1. Select **Configure > Switch > Save**.

The **Save Switch Configurations** dialog box displays (Figure 81).



**FIGURE 81** Save switch configurations

2. Select the switches for which you want to save configuration files from **Available Switches**.
3. Click the right arrow to move the selected switches to **Selected Switches**.
4. Click **OK**.

Configuration files from the selected switches are saved to the repository.

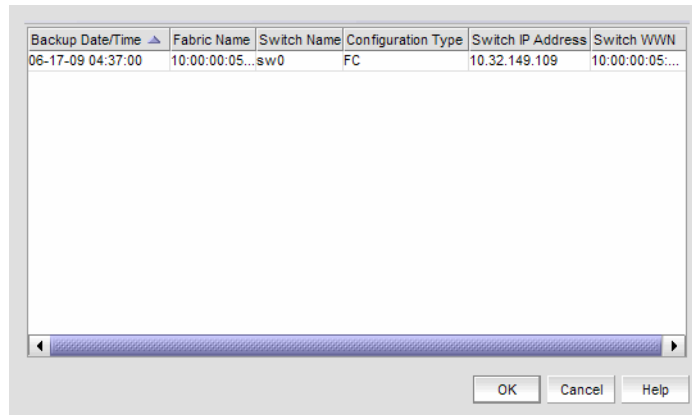
## Restoring a switch configuration for a selected device

The **Restore Switch Configuration** dialog box enables you to download a previously saved switch configuration to a selected device.

To restore a switch configuration, complete the following steps.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Restore**.

The **Restore Switch Configuration** dialog box displays (Figure 81).



**FIGURE 82** Restore Switch Configuration dialog box

2. Select the switch configuration you want to download from the **Saved Switch Configurations** table.
3. Click **OK**.

The configuration is downloaded to the device. If necessary, the restoration process prompts you to disable and reboot the device before the configuration begins. This lets you determine whether the configuration backup should be performed immediately or at a later time.

When you restore a switch configuration on a Virtual Fabrics-configured chassis, the configuration data for the logical switches is downloaded to the switch as configured in the file. When you restore a switch configuration on a logical switch, only the selected logical switch configuration data is downloaded to the switch.

## Backing up a switch configuration

**NOTE**  
The Enhanced Group Management (EGM) license must be activated on a switch to perform this procedure and to use the supportSave module.

If a periodic backup is scheduled at the SAN level, that backup will apply to all switches from all fabrics discovered. Any new fabrics being discovered are automatically added to the list of fabrics to be backed up.

**NOTE**  
If a backup is scheduled for more than one fabric and some of the fabrics contain common members, the backup will include the unique switch configuration values obtained from the fabrics.

You can schedule a backup of one or more switch configurations. The configuration files are stored in the Management application database.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Schedule Backup**.

The **Schedule Backup of Switch Configurations** dialog box displays (Figure 83).

☒ Enable scheduled backup

Schedule

Frequency: Daily

Day: Tuesday

Hour: 10 Minute: 15

Time: 10:15

Purge Backups: 30 days and older

Scope - Includes all switches discovered at time of backup

☒ Backup all fabrics

Selected Fabrics

Backup	Fabric Name	Status	# of Switches
<input checked="" type="checkbox"/>	10:00:00:05:1E:34:D...	Down	1
<input checked="" type="checkbox"/>	10:00:00:05:1E:35:3...	Marginal	1
<input checked="" type="checkbox"/>	10:00:00:05:1E:37:B...	Unreachable	1

OK Cancel Help

**FIGURE 83** Schedule backup of switch configurations

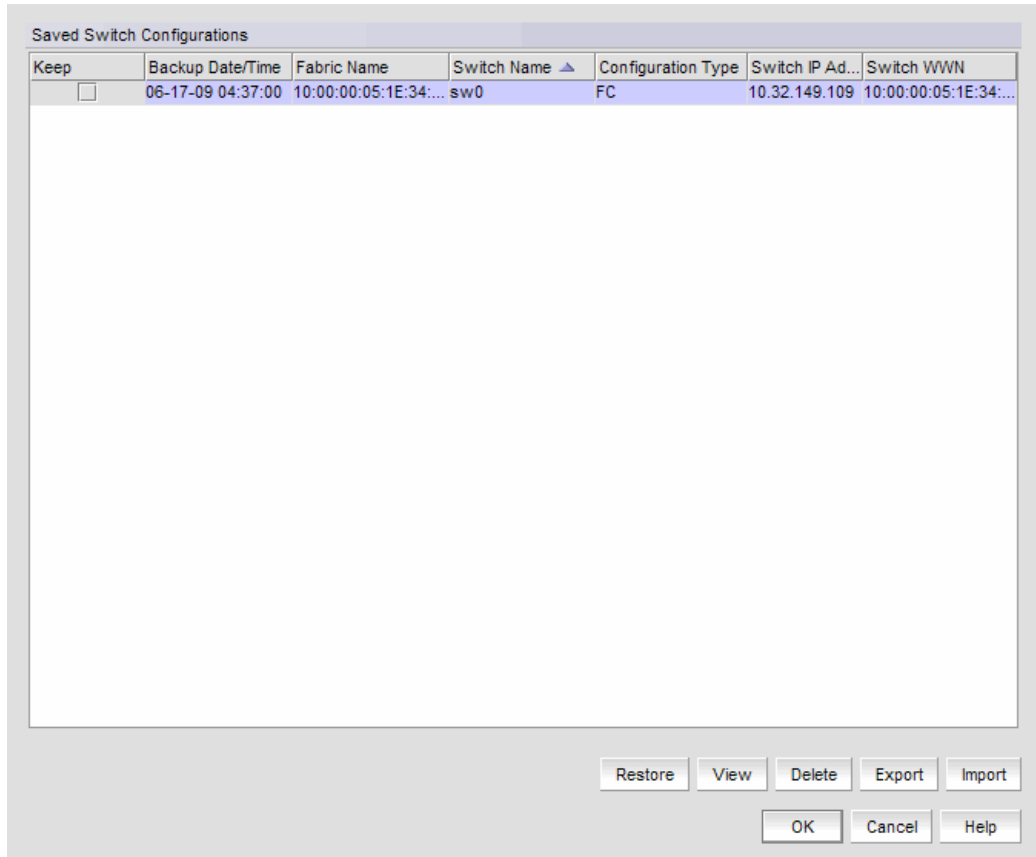
2. Click the **Enable scheduled backup** check box.

3. Set the **Schedule** parameters. These include the following:
  - The desired **Frequency** for backup operations (daily, weekly, monthly).
  - The **Day** you want back up to run.  
If **Frequency** is **Daily**, the Day list is grayed out.  
If **Frequency** is **Weekly**, choices are days of the week (Sunday through Saturday).  
If **Frequency** is **Monthly**, choices are days of the month (1 through 31).
  - The **Time** (hour, minute) you want back up to run.
  - The maximum age allowed before you **Purge Backups**.  
The number of purge days should be at least one day more than the selected backup frequency.  
The backup purge thread runs every day at 12:30 PM and deletes all back up configurations that exceed the maximum age allowed.
4. Choose one of the following options to determine the scope of the backup.
  - Select the **Backup all fabrics** check box, if necessary, to back up all switch configurations of discovered switches in all fabrics
  - Clear the **Backup all fabrics** check box and select the specific fabric check boxes in the **Selected Fabrics** table to back up individual fabrics.  
If any switches do not have the EGM license, a messages displays. Click **OK** to enable backup on the switches with the EGM license.
5. Click **OK**.  
Click **OK** on the confirmation message.

## Restoring a configuration from the repository

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

The **Switch Configuration Repository** dialog box displays (Figure 84).



**FIGURE 84** Switch Configuration Repository

2. Select the configuration you want to restore, and click **Restore**.

The configuration is downloaded to the device. If necessary, the restoration process prompts you to disable and reboot the device before the configuration begins. This lets you determine whether the configuration backup should be performed immediately or at a later time.

If you confirm the restoration, the entire configuration is restored; you cannot perform selective download for specific configuration sections.

## Viewing configuration file content

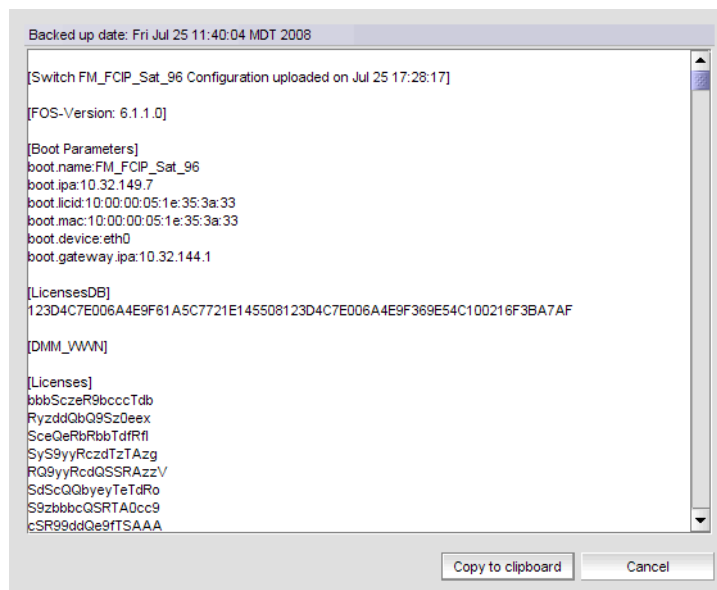
You can view switch configuration file content in a text file.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

The **Switch Configuration Repository** dialog box displays.

2. Click **View**.

The configuration details display. If you want to save the contents as a text file, click **Copy to Clipboard**, paste the copy into a text editor (Notepad or Wordpad on Windows systems), and save the file.



**FIGURE 85** Configuration file content

3. Click **Close** to close the dialog box.
4. Click **Yes** on the message.

## Searching the configuration file content

To search the configuration file content, complete the following steps.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

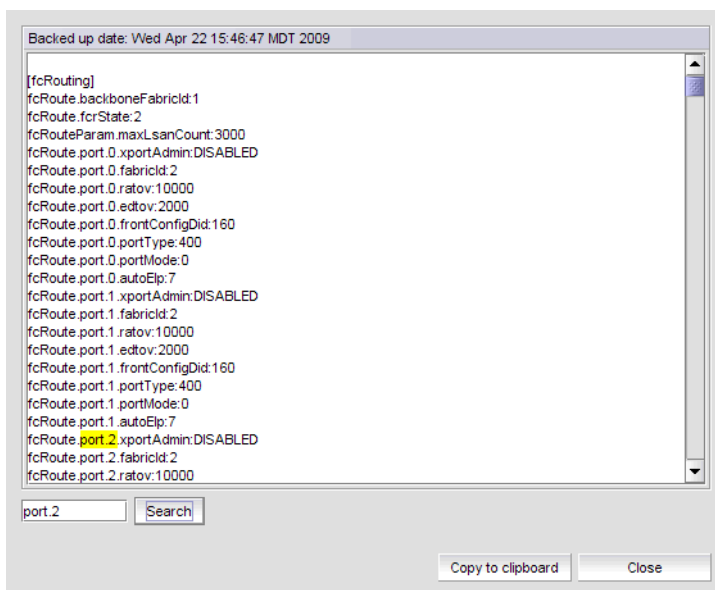
The **Switch Configuration Repository** dialog box displays.

2. Click **View**.

The configuration details display.

3. Enter the information you want to search for in the field and click **Search**.

The text string you are searching for is highlighted in the dialog box. Continue clicking **Search** to scroll through the contents until you find the information you need. If the search item is not found a 'not found' message displays. Click **OK** to close the message.



**FIGURE 86** Configuration file content

4. Click **Close** to close the dialog box.
5. Click **Yes** on the message.

## Deleting a configuration

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

The **Switch Configuration Repository** dialog box displays.

2. Select the configuration you want to delete, and click **Delete**.

## Exporting a configuration

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

The **Switch Configuration Repository** dialog box displays.

2. Select the configuration you want to export, and click **Export**.

The file chooser appropriate to your operating system displays.

3. Use the file chooser to select the location into which you want to export the configuration.
4. Click **Export**.

The configuration is automatically named (*Device\_Name\_Date\_and\_Time*) and exported to the location you selected.

## Importing a configuration

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

The **Switch Configuration Repository** dialog box displays.

2. Click **Import**.

The file chooser appropriate to your operating system displays.

3. Use the file chooser to select the file from which you want to import the configuration, and click **Import**.

## Keeping a copy past the defined age limit

1. Right click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

The **Switch Configuration Repository** dialog box displays.

2. Select the check box under **Keep** for the configuration you want to preserve. The configuration will be kept until it is manually deleted, or until the **Keep** check box is cleared to enable the age limit again.
3. Click **OK**.

## Replicating configurations

You can replicate a switch SNMP configuration, the Fabric Watch configuration, Trace Destination configuration, or the entire configuration.

Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Replicate > Configuration**.

A wizard is launched to guide you through the process.

## Replicating security configurations

You can replicate an AD/LDAP Server, DCC, IP, RADIUS Server, or SCC security policy.

Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Replicate > Security**.

A wizard is launched to guide you through the process.

## Device properties

You can customize the device **Properties** dialog boxes to display only the data you need by adding, editing, and deleting property labels. You can also edit property fields to change information.

### Viewing properties

To view the properties for a device or fabric, complete the following step.

Right-click any product icon and select **Properties**.

The **Properties** dialog box displays, with information related to the selected device (such as, switches, directors, HBAs, trunks, tunnels, and nodes).

Depending on the device type, any of the following port tabs may display:

- FC Ports
- GigE Ports
- IP Ports
- iSCSI Ports
- POM
- Remote Ports
- SFP
- Virtual Sessions Ports
- Virtual FCoE Ports

Depending on the device type, some of the properties listed in the following table may not be available for all products.

**TABLE 10** Device properties

Field/Component	Description
<b>Addressing Mode</b>	The addressing mode of the switch.
<b>Back to Edge Routing Support</b>	Whether back to edge routing is supported.
<b>Bandwidth</b>	The bandwidth of the FCIP tunnel.
<b>Capability</b>	The node capability.
<b>Compression</b>	Whether compression is On or Off for the FCIP tunnel.
<b>Connected Virtual FCoE Port</b>	The fabric name, switch name, and virtual FCoE port number of the connected virtual FCoE port.
<b>Contact</b>	The primary contact at the customer site.

**TABLE 10** Device properties (Continued)

Field/Component	Description
Contributors	The device contributors.
Device Type	Whether the device is an initiator or target.
Description	A description of the customer site.
Destination IP Address	The IP address of the of the FCIP tunnel destination device.
Discovery Status	The discovery status of the switch. Examples include 'Discovered: Seed Switch' and 'Discovered: Not Reachable'.
Domain ID	The device's domain ID, which is the top-level addressing hierarchy of the domain.
Fabric	The fabric name.
Fabric Name	The name specified through the device Element Manager.
Fabric Watch	Whether Fabric Watch is up or down.
Fastwrite	Whether fastwrite is On or Off for the FCIP tunnel.
FC Port	The FC port of the FCIP tunnel.
FCoE Capable	Whether the device is Fibre Channel over Ethernet capable.
FCS Role	Whether FCS is supported.
Firmware	The firmware version.
GigE Port	The GigE port of the FCIP tunnel.
Host Name	The Host name.
IKE Policy #	The IKE policy number. Also includes the following information: <ul style="list-style-type: none"> <li>• Authentication Algorithm</li> <li>• Encryption Algorithm</li> <li>• Diffie-Hellman</li> <li>• SA Life</li> </ul>
IP Address	The device's IP address.
IPSec Policy #	The IPSec policy number. Also includes the following information: <ul style="list-style-type: none"> <li>• Authentication Algorithm</li> <li>• Encryption Algorithm</li> <li>• SA Life</li> </ul>
L2 Capable	Whether the device is Layer 2 capable.
L3 Capable	Whether the device is Layer 3 capable.
L2 Mode	The Layer 2 mode. Options include Access, Converged, or Trunk.
LAG ID	The link aggregation group identifier.
Last Discovery	The date and time of the last discovery.
Location	The customer site location.
MAC address	In a network, the Media Access Control (MAC) address is a unique number that identifies a specific hardware interface. It is a 12-digit hexadecimal number.
Managed By	The management program used to manage the fabric.
Master Port	The master port of the trunk.

**TABLE 10** Device properties (Continued)

Field/Component	Description
Member Ports	The member ports of the trunk.
Model	The model number of the device.
Name	The user-defined name of the switch.
Node Name	The name of the node.
Node WWN	The world wide name of the node.
Physical/Logical	Whether the device is a physical device or a logical device.
Port Count	The number of ports.
Port Type	The port type.
Preshared key configured	Whether the preshared key is configured for the FCIP tunnel.
Reason	The device status.
Remote Switch Name	The remote switch name of the trunk.
Remote Switch IP	The remote switch IP address of the trunk.
Remote Switch WWN	The remote switch world wide name of the trunk.
Remote Slot #	The remote slot number of the trunk.
Remote Master Port	The remote master port of the trunk.
Remote Member Ports	The remote member port of the trunk.
Sequence number	The sequence number of the switch.
Serial #	The hardware serial number.
Slot #	The slot number of the trunk.
Source IP Address	The IP address of the of the FCIP tunnel source device.
Speed (Gb/s)	The speed of the port in gigabytes per second.
State	The device's state, for example, online or offline.
Status	The operational status.
Switch Name	The switch name.
Switch IP	The switch IP address.
Switch WWN	The switch world wide name.
Tape Pipelining	Whether tape pipelining is On or Off for the FCIP tunnel.
Tunnel ID	The tunnel identifier.
Type	The device type.
Unit Type	The unit type of the node.
Vendor	The product vendor.
# Virtual FCoE port count	The number of virtual FCoE ports on the device. There is a one-to-one mapping of TE ports to virtual FCoE ports. Therefore, the number of virtual session ports is one for directly connected devices.
VLAN #	The VLAN number of the FCIP tunnel.
VLAN Class of Service for Control Connection	The VLAN class of service for the control connection of the FCIP tunnel.

**TABLE 10** Device properties (Continued)

Field/Component	Description
VLAN Class of Service for Data Connection	The VLAN class of service for the data connection of the FCIP tunnel.
VLAN ID	The VLAN identification number.
WWN	The world wide name of the device.

## Adding a property label

You can add a new field to any of the tabs on the **Properties** dialog box. To add a new field, complete the following steps.

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab to which you want to add a property.
3. Right-click on any label.  
The new property label displays above the one you select.
4. Select **Add**.  
The **Add Property** dialog box displays.
5. Type a label and description for the property.
6. Select the property type from the **Type** list, if available.
7. Click **OK**.  
The new property displays above the one you selected.

## Editing a property label

You can edit any label that you create on the **Properties** dialog box.

To edit any field you create, complete the following steps.

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to edit a property.
3. Right-click the label for the property you want to edit.
4. Select **Edit**.  
The **Edit Property** dialog box displays.
5. Change the label and description for the property, as needed.
6. Change the property type from the **Type** list, if available.
7. Click **OK**.

### Deleting a property label


You can delete any label that you created on any of the tabs from the **Properties** dialog box. To delete a label, complete the following steps.

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to delete a property.
3. Right-click the label for the property you want to delete.
4. Select **Delete**.
5. Click **Yes** on the confirmation message.

The property you selected is deleted.

### Editing a property field

You can edit fields on the **Properties** dialog box. To edit a field, complete the following steps.

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to edit a field.  
Fields containing a green triangle (  ) in the lower right corner are editable.
3. Click in an editable field and change the information.
4. Click **OK**.

## Enhanced group management

Use Enhanced Group Management (EGM), a separate licensed feature, to control access to specific features on Fabric OS devices. The features affected include the following:

- **Firmware Download** - enables you to perform group firmware download.  
For specific instructions for firmware download, refer to [“Firmware management”](#) on page 197.
- **Security** - enables you to perform Group Security Policy Replication.  
For specific instructions for security, refer to [“Configuration repository management”](#) on page 183.
- **Configuration Management** - enables you to perform Group Configuration Upload and Replication.  
For specific instructions for configuration management, refer to [“Replicating configurations”](#) on page 191.

## Firmware management

A firmware file repository (Windows systems only) is maintained on the server in the following location: C:\Program Files\Install\_Directory\data\ftproot\6.1.1\n.n.n\n.n.n\

The firmware repository is used by the internal FTP server that is delivered with the Management application software, and may be used by an external FTP server if it is installed on the same platform as the Management application software. The repository is not available to FTP servers on external platforms. The repository is used only for Fabric OS firmware. M-EOS firmware is handled through the Element Manager specific to the switch or director model.

---

**NOTE**

Non-disruptive firmware download (HCL) is not supported when downgrading from Fabric OS version 6.2 to 6.1. You must remove all non-default logical switches and disable Virtual Fabrics before downgrading.

---

---

**NOTE**

Firmware download is not supported in pure IPv6 mode.

---

---

**NOTE**

You cannot use Fabric OS firmware download with command line options in the Management application.

---

### Displaying the firmware repository

The firmware repository is available on the **Firmware Management** dialog box. The Management application supports .zip and .gz compression file types for firmware files.

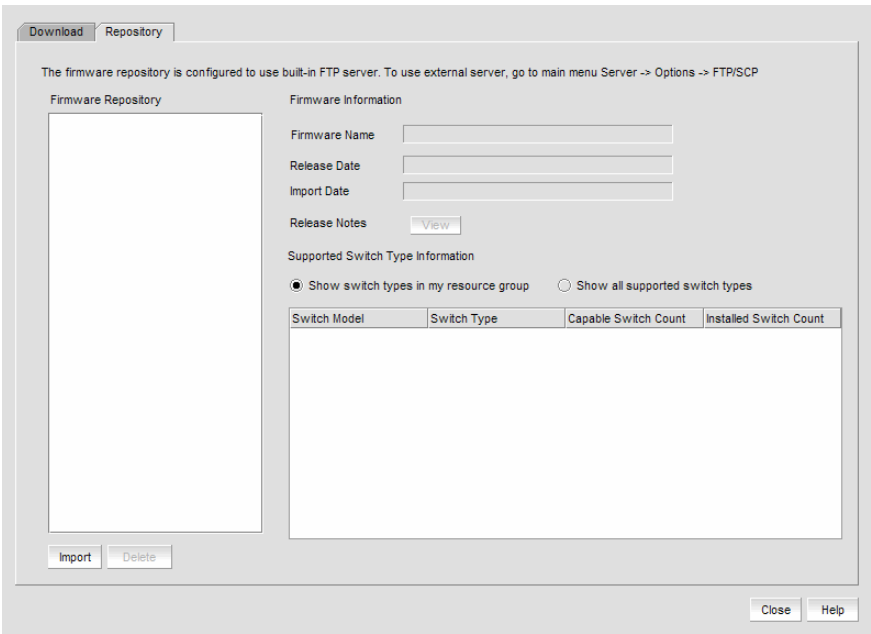
1. Select **Configure > Firmware Management**.

The **Firmware Management** dialog box displays.

2. Select the **Repository** tab ([Figure 87](#)).

Initially, the repository is empty. You must import firmware files into the repository. Imported firmware files are then displayed under **Firmware Repository**.

# 8 Importing a firmware file and release notes



**FIGURE 87** Firmware repository

3. View information about a specific firmware file by selecting the firmware file in the **Firmware Repository**.

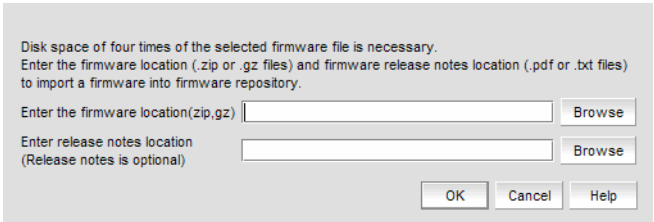
The **Firmware Name**, **Release Date**, and **Import Date** are displayed. You may also view the **Release Notes**, if the release notes were imported.

## Importing a firmware file and release notes

Firmware files and release notes can be imported into the Firmware Repository.

1. Select **Configure > Firmware Management**.  
The **Firmware Management** dialog box displays.
2. Select the **Repository** tab (Figure 87).
3. Click **Import**.

The **Import Firmware from File** dialog box displays (Figure 88).



**FIGURE 88** Import firmware

4. Type in the location of the firmware file and release notes, or use **Browse** to select the location.  
The Management application supports .zip and .gz compression file types for firmware files.
5. Click **OK**.  
You return to the **Repository** tab. The file is listed in the Firmware Repository when the import is complete and successful.

## Deleting a firmware file

Firmware files can be deleted from the Firmware Repository.

1. Select **Configure > Firmware Management**.  
The **Firmware Management** dialog box displays.
2. Select the **Repository** tab (Figure 87).
3. Select one or more firmware files from the Firmware Repository for deletion.
4. Click **Delete**.

A confirmation dialog displays. Click **Yes** to confirm. The firmware file is deleted from the repository.

## Download firmware

---

### NOTE

Non-disruptive firmware download (HCL) is not supported when downgrading from Fabric OS version 6.2 to 6.1. You must remove all non-default logical switches and disable Virtual Fabrics before downgrading.

---

---

### NOTE

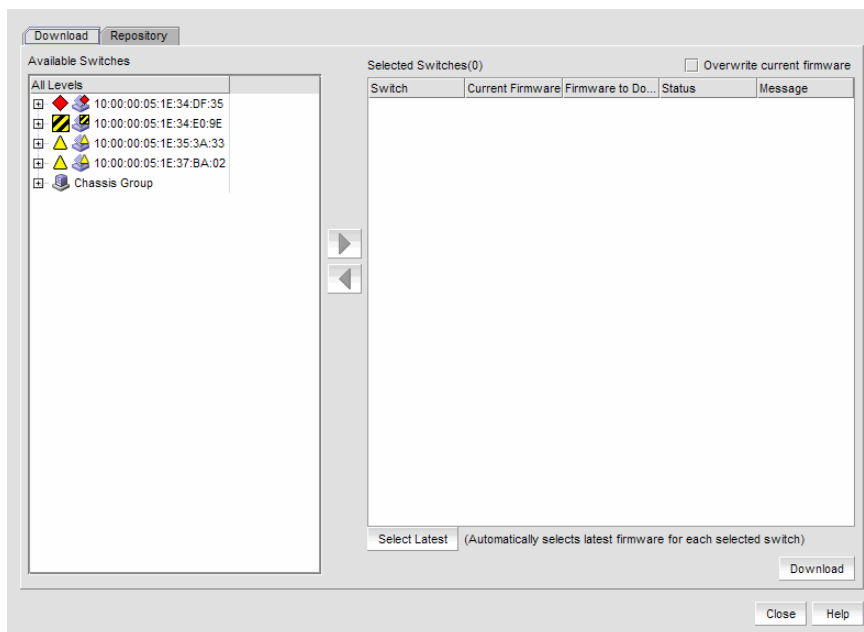
You cannot use Fabric OS firmware download with command line options in the Management application.

---

You can download firmware using the **Firmware Management** dialog box.

1. Select **Configure > Firmware Management**.  
The **Firmware Management** dialog box displays.
2. Select the **Download** tab (Figure 89).

## 8 Download firmware



**FIGURE 89** Firmware download

3. Select one or more switches from **Available Switches**.
4. Click the right arrow to move the switches to **Selected Switches**.
5. Select a specific version from the **Firmware to Download** column, or use **Select Latest** to automatically select the latest version.

If you have your FTP or SCP Server configured to use an external FTP or SCP Server, the **Firmware to Download** column is empty.

6. If you want to overwrite the current firmware, even if the selected version is the same as the version currently running on the switch, click the **Overwrite Current Firmwares** check box.
7. If you configured an external server, choose from one of the following options:
  - Select **External FTP Server** to download from the external FTP server.  
If you select external FTP server, configure the following on the FTP server:
    - ☐ Create user and password.
    - ☐ Select the **Shared folders** link and set firmware location as the home directory and select all check boxes under the **Files** and **Directories** attributes.
  - Select **SCP Server** to download from the external SCP server.

8. If you configured an external server, enter the path to the firmware directory in the **Firmware Directory** field.

This field does not display if the external server is installed on the same machine as the Management application and occupies port 21.

9. Click **Download**.

While the firmware is downloaded to the device, the **Status** column displays the current download status. Once firmware download is complete, the **Message** column displays whether the download was a success or failure.

## Host port mapping

HBAs and Hosts discovered through a fabric can be easily identified in the topology by their product icons. For a list of products and their icons, refer to [“Product icons”](#) on page 11. Once identified in the topology, you can create Hosts and assign the HBAs to them and import an externally created Host port mapping file (.CSV) to the Management application.

### NOTE

The Management application now enables you to map HBAs from multiple fabrics (previous versions limited HBA mapping to one fabric).

The Management application also enables you to discover Hosts directly using Host discovery (for step-by-step instructions, refer to [“Host discovery”](#) on page 42). If you discover a Host directly, when you open the **Host Port Mapping** dialog box the Management application automatically groups all HBAs under the discovered Host.

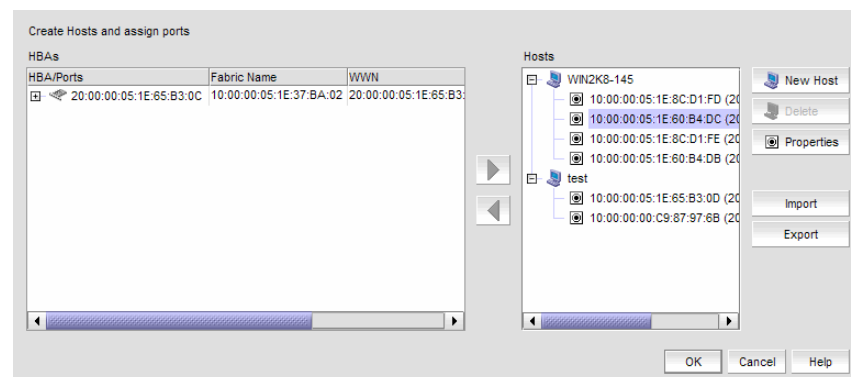
If you create a new Host and associate HBAs to it, then you try to discover a Host with the same HBAs using Host discovery, the HBA's discovered using Host discovery must match the HBAs associated to the Host exactly; otherwise, Host discovery will fail.

## Creating a new Host

To create a new Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

The **Host Port Mapping** dialog box displays.



**FIGURE 90** Host Port Mapping dialog box

2. Click **New Host**.

A new Host displays in the **Hosts** table in edit mode.

3. Double-click the new Host name to make it editable, type a name for the new Host, and press **Enter**.

The name of the new Host appears in the **Hosts** table in alphabetical order. To assign HBAs to this Host, refer to [“Associating an HBA with a Host”](#) on page 203.

4. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

## Renaming an HBA Host

To rename a Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.  
The **Host Port Mapping** dialog box displays.
2. Click the Host you want to rename in the **Hosts** table, wait a moment, and then click it again.  
The Host displays in edit mode.
3. Type a new name for the Host.  
The name of the Host appears in the **Hosts** table in alphabetical order with the new name. To assign HBAs to this Host, refer to [“Associating an HBA with a Host”](#) on page 203.
4. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

## Deleting an HBA Host

To delete a Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.  
The **Host Port Mapping** dialog box displays.
2. Select the Host you want to delete in the **Hosts** table.
3. Click **Delete**.  
The selected Host is deleted. Any HBAs associated with the Host are automatically moved from the **Host** table to the **HBAs** table.
4. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

## Viewing Host properties

To view Host properties, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.  
The **Host Port Mapping** dialog box displays.
2. Select the HBA Host port you want to view in the **Hosts** table.
3. Click **Properties**.  
The **Properties** dialog box for the selected port displays.
4. Click **OK** to close the **Properties** dialog box.
5. Click **OK** to close the **Host Port Mapping** dialog box.

## Associating an HBA with a Host

### ATTENTION

Discovered information overwrites your user settings.

To associate an HBA with a Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.  
The **Host Port Mapping** dialog box displays.
2. Select the Host to which you want to assign HBAs in the **Hosts** table or click **New Host** to create a new Host.
3. Select the HBA from the **HBAs** table on the left and click the right arrow.  
The HBA displays in the **Hosts** table. The HBA is now associated with the selected Host.
4. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.  
On the Connectivity Map, the HBA displays in the Host.

## Importing HBA-to-Host mapping

The **Host Port Mapping** dialog box enables you to import externally created HBA ports-to-Host mapping information into the application. The imported file must be in CSV format. The first row must contain the headers (wwn, name) for the file.

### Example

```
wwn,name
20:00:00:00:C9:69:D5:27, s1
20:00:00:05:1E:0A:35:0E, s2
```

When the import is complete a result summary displays with the information listed in [Table 11](#).

**TABLE 11** Import Results

Value	Definition
Total Valid Input Records	Number of lines identified in the CSV file without any errors (excluding the Header).
Unique HBA WWNs Recognized	Number of unique HBAs identified in the CSV file.
Hosts Created or Identified	Number of Hosts identified in the CSV file already discovered, and which are either online or offline but not deleted.
Conflicting HBA Mappings	Number of occurrences where you were asked to decide whether to override previously discovered information. If you select Yes to All, or No to All, each occurrence where conflict resolution occurs automatically is counted as one conflict.
Overwritten HBA Mappings	Number of times a previously discovered mapping is overwritten during the import process.
Importing Errors	Number of errors encountered during the import.
Details	Tabulates the error information with respect to the line number where it occurred.

To import Host port mapping, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

The **Host Port Mapping** dialog box displays.

2. Click **Import**.

The **Import** dialog box displays.

3. Browse to the file (CSV format only) you want to import.

4. Click **Open** on the **Import** dialog box.

The file imports, reads, and applies all changes line-by-line and performs the following:

- Checks for correct file structure and well-formed WWNs, and counts number of errors.  
If more than 5 errors occur, import fails and a 'maximum error count exceeded' message displays. Edit the Host port mapping file and try again.
- Checks for duplicate HBAs.  
If duplicates exist, a message displays with the duplicate mappings detailed. Click **Yes** to continue. Click **No** to edit the Host port mapping file and try again.
- Checks for existing mappings in the current map.  
If a mapping already exists, a message displays with the current mapping information. Click **Yes** to overwrite the current mapping. Click **Yes to All** to overwrite all mapping conflicts. Click **No** to leave the current mapping. Click **No to All** to leave all current mappings when conflict occurs. Click **Cancel** to cancel the import.

5. Click **OK** to close the **Import Results** dialog box.

6. Click **OK** to close the **Host Port Mapping** dialog box.

## Removing an HBA from a Host

To remove an HBA from a Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

The **Host Port Mapping** dialog box displays.

2. Select the HBA from the **Hosts** table on the right and click the left arrow.

The HBA you selected is removed from the **Hosts** table and the HBA is no longer associated with the Host.

3. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

On the Connectivity Map, the HBA displays on its own.

## Exporting Host port mapping

The **Host Port Mapping** dialog box enables you to export a Host port. The export file uses the CSV format. The first row contains the headers (HBA/Ports WWN, Host Name) and the switch to which the port is connected.

### Example

```
HBA World Wide Name, Host Name
5005076717011E7D, Server1
50050767170A5AAF, Server1
```

To export a Host port, complete the following steps.

1. Open the **Host Port Mapping** dialog box by performing one of the following actions:

- Select an HBA port icon in the topology view, then select **Discover > Host Port Mapping**.
- Right-click any HBA port icon in the topology view and select **Host Port Mapping**.
- Right-click any HBA port in the Device Tree and select **Host Port Mapping**.

The **Host Port Mapping** dialog box displays.

2. Select the Host port you want to export from the **HBA/Ports** list.

To configure Host port mapping, refer to [“Creating a new Host”](#) on page 201 and [“Associating an HBA with a Host”](#) on page 203.

3. Click **Export**.

The **Export** dialog box displays.

4. Browse to the location where you want to save the export file.

Depending on your operating system, the default export location are as follows:

- Desktop\My documents (Windows)
- \root (Linux)
- \ (Solaris)

5. Enter a name for the files and click **Save**.

6. Click **OK** to close the **Host Port Mapping** dialog box.

# Ports

You can enable and disable ports, as well as view port details, properties, type, status, and connectivity.

## Viewing port connectivity

The connected switch and switch port information displays for all ports.

To view port connectivity, choose one of the following steps:

- Right-click a product icon and select **Port Connectivity**.
- Select a product icon and select **Monitor > Port Connectivity**.

The **Port Connectivity View** dialog box displays (Figure 91).

Fabric: 10.00.00.05:1E:34:DF:35, Switch Name: switch\_128\_11

Port Number	Blade Number	Port Name	User Port Number (Hex)	Area ID (Hex)/Port Index (Hex)	FC Address	Port WWN	Status	Stat
7	N/A		7	0x07	0x0A0700	20:07:00:05:1E:34:DF:35	Healthy	Offl
14	N/A		14	0x0E	0x0A0E00	20:0E:00:05:1E:34:DF:35	Healthy	Offl
27	N/A		27	0x1B	0x0A1B00	20:1B:00:05:1E:34:DF:35	Healthy	Offl
2	N/A		2	0x02	0x0A0200	20:02:00:05:1E:34:DF:35	Healthy	Offl
4	N/A		4	0x04	0x0A0400	20:04:00:05:1E:34:DF:35	Healthy	Offl
23	N/A		23	0x17	0x0A1700	20:17:00:05:1E:34:DF:35	Healthy	Onli
5	N/A		5	0x05	0x0A0500	20:05:00:05:1E:34:DF:35	Healthy	Offl
16	N/A		16	0x10	0x0A1000	20:10:00:05:1E:34:DF:35	Healthy	Offl
30	N/A		30	0x1E	0x0A1E00	20:1E:00:05:1E:34:DF:35	Healthy	Offl
17	N/A		17	0x11	0x0A1100	20:11:00:05:1E:34:DF:35	Healthy	Offl
8	N/A		8	0x08	0x0A0800	20:08:00:05:1E:34:DF:35	Healthy	Offl
3	N/A		3	0x03	0x0A0300	20:03:00:05:1E:34:DF:35	Healthy	Offl
28	N/A		28	0x1C	0x0A1C00	20:1C:00:05:1E:34:DF:35	Healthy	Offl
9	N/A		9	0x09	0x0A0900	20:09:00:05:1E:34:DF:35	Healthy	Offl
18	N/A		18	0x12	0x0A1200	20:12:00:05:1E:34:DF:35	Healthy	Offl
22	N/A		22	0x16	0x0A1600	20:16:00:05:1E:34:DF:35	Healthy	Offl
13	N/A		13	0x0D	0x0A0D00	20:0D:00:05:1E:34:DF:35	Healthy	Offl
24	N/A		24	0x18	0x0A1800	20:18:00:05:1E:34:DF:35	Healthy	Offl
12	N/A		12	0x0C	0x0A0C00	20:0C:00:05:1E:34:DF:35	Healthy	Offl
21	N/A		21	0x15	0x0A1500	20:15:00:05:1E:34:DF:35	Healthy	Offl
29	N/A	Port No 29	29	0x1D	0x0A1D00	20:1D:00:05:1E:34:DF:35	Healthy	Onli
29	N/A	Port No 29	29	0x1D	0x0A1D00	20:1D:00:05:1E:34:DF:35	Healthy	Onli
29	N/A	Port No 29	29	0x1D	0x0A1D00	20:1D:00:05:1E:34:DF:35	Healthy	Onli
19	N/A		19	0x13	0x0A1300	20:13:00:05:1E:34:DF:35	Healthy	Offl
10	N/A		10	0x0A	0x0A0A00	20:0A:00:05:1E:34:DF:35	Healthy	Offl
6	N/A		6	0x06	0x0A0600	20:06:00:05:1E:34:DF:35	Healthy	Offl
31	N/A		31	0x1F	0x0A1F00	20:1F:00:05:1E:34:DF:35	Healthy	Offl
26	N/A		26	0x1A	0x0A1A00	20:1A:00:05:1E:34:DF:35	Healthy	Offl
15	N/A		15	0x0F	0x0A0F00	20:0F:00:05:1E:34:DF:35	Healthy	Offl
20	N/A		20	0x14	0x0A1400	20:14:00:05:1E:34:DF:35	Healthy	Offl
1	N/A	Port 1	1	0x01	0x0A0100	20:01:00:05:1E:34:DF:35	Healthy	Offl

**FIGURE 91** Port Connectivity View dialog box

Loop devices are displayed in multiple rows, one row for each related device port.

If no switch or device is connected to the port, then the related fields are empty.

The following table details the information located (in alphabetical order) on the **Port Connectivity View** dialog box.

**TABLE 12** Port connectivity properties

Field	Description
<b>Actual Distance</b>	The actual distance for end-to-end port connectivity.
<b>Area ID (Hex)</b>	The area ID (in hexadecimal) of the port.
<b>Blade Number</b>	The number of the blade.
<b>Blocked</b>	Whether the selected port is blocked.

**TABLE 12** Port connectivity properties (Continued)

Field	Description
Buffer Limited	Whether buffers are limited.
Buffers Needed/Allocated	The ratio of buffers needed relative to the number of buffers allocated.
Calculated Status	The operational status. There are four possible operation status values: <ul style="list-style-type: none"> <li>• Up - Operation is normal.</li> <li>• Down - The port is down or the route to the remote destination is disabled.</li> <li>• Disabled - The connection has been manually disabled.</li> <li>• Backup Active - The backup TCP port is active due to a failover.</li> </ul>
Capability	The device capability of the connected device port. The value is mapped depending on whether it is a name server (NS) or a FICON device.
Connected Blade Number	The number of the connected blade.
Connected Port Area ID (Hex) Port Index (Hex)	The area ID and the port index (both in hexadecimal) of the connected port.
Connected Port Name	The name of the connected port.
Connected Port Number	The number of the connected port.
Connected Port Speed	The speed of the connected port.
Connected Port Status	The connection status. There are four possible operation status values: <ul style="list-style-type: none"> <li>• Up - Operation is normal.</li> <li>• Down - The port is down or the route to the remote destination is disabled.</li> <li>• Disabled - The connection has been manually disabled.</li> <li>• Backup Active - The backup TCP port is active due to a failover.</li> </ul>
Connected Port State	The connected port's state; for example, online or offline.
Connected Port WWN	The world wide name of the connected port.
Connected User Port Number (Hex)	The port number (in hexadecimal) of the connected user port.
COS	The class of service (CoS) value, which ranges between zero (low priority) and seven (high priority).
Device Node WWN	The world wide name of the device node.
Device Symbolic Name	The symbolic name of the device node.
Device Port/Switch Domain ID	The device port and switch domain ID.
Device Port/Switch WWN	The device port and switch world wide name.
Device Port/Switch Name	The device port and switch name.
Device Port/Switch State	The device port and switch state.
Device Port/Switch Manufacturer	The device port and manufacturer of the switch.
Device Port/Switch Manufacturing Plant	The device port and switch manufacturing plant.
Device Port / Switch Type Number	The device port and switch type number.

**TABLE 12** Port connectivity properties (Continued)

Field	Description
Device Type	The device type; for example, target or initiator.
FC4 Type	The active FC4 type; for example, SCSI.
FC Address	The Fibre Channel address. Each FC port has both an address identifier and a world wide name (WWN).
Flag	Whether a flag is on or off.
Hard Address	The hard address of the device.
Host Name	The name of the Host.
Long Distance	Whether the connection is considered to be normal or longer distance.
Model	The model name and number of the device.
Parameter	Device parameters.
Physical/Virtual/NPIV	Whether the port is a physical port, a virtual port, or an NPIV_port.
Port Address	The port's address.
Port IP Address	The port's IP address.
Port Module	The port's module.
Port Name	The port's name.
Port Number	The port's number.
Port Type	The type of port; for example, U_Port (universal port) or FL_Port (Fabric loop port).
Port WWN	The world wide name of the port.
Prohibited	Whether the allow/prohibit matrix is activated.
Serial #	The port's serial number.
Speed	The current port speed, in gigabits per second.
State	The port's state; for example, online or offline.
Switch Dynamic Load Sharing	Whether switch dynamic load sharing is enabled.
Switch FCS Role	Whether the Fabric Configuration Server (FCS), which is the primary point of control that manages all the switches within a fabric, is enabled.
Switch FMS mode	Whether the File Management Solution (FMS) mode is enabled.
Switch Has Certificate	Whether the switch has a certificate (true or false).
Switch IDID	Whether the switch's insistent domain ID (IDID) is enabled. If it is enabled, the IDID is the same ID that is requested during switch reboots, power cycles, CP failovers, firmware downloads, and fabric reconfiguration.
Switch in Order Delivery	Whether switch in-order delivery is enabled.
Switch IP	The switch's IP address.
Switch Port Count	The number of ports on the switch.
Switch Role	The role of the switch; for example, subordinate.

**TABLE 12** Port connectivity properties (Continued)

Field	Description
Switch Routing Policy	Whether a routing policy, for example, port-based routing policy, is enabled.
Switch Secure Mode	Whether switch secure mode is enabled.
Switch Status	The operational status. There are four possible operation status values: <ul style="list-style-type: none"> <li>• Up - Operation is normal.</li> <li>• Down - The port is down or the route to the remote destination is disabled.</li> <li>• Disabled - The connection has been manually disabled.</li> <li>• Backup Active - The backup TCP port is active due to a failover.</li> </ul>
Switch Supplier Serial Number	The serial number of the switch supplier.
Switch Version	The switch's version number.
Tag	The tag number of the port.
Unit Type	The switch unit type.
User Port Number	The port number of the user's device.
Vendor	The hardware vendor's name.

## Refreshing the port connectivity view

To obtain configuration changes that occurred since the **Port Connectivity View** dialog box opened, click **Refresh**.

## Enabling a port

To enable a port from the port connectivity view, right-click the port you want to enable from the **Port Connectivity View** dialog box and select **Disable/Enable Port > Enable**.

## Disabling a port

To disable a port from the port connectivity view, right-click the port you want to disable from the **Port Connectivity View** dialog box and select **Disable/Enable Port > Disable**.

## Filtering port connectivity

To filter results from the port connectivity view, complete the following steps.

1. Click the **Filter** link from the **Port Connectivity View** dialog box

The **Filter** dialog box displays (Figure 92).

Field	Relation	Value	Operator
Port Number	contains	1	AND
			AND
			AND
			AND
			AND
			AND
			AND
			AND
			AND

Reset OK Cancel

**FIGURE 92** Filter dialog box

2. Click a blank cell in the **Field** column to select the property from which to filter the results.
3. Click a blank cell in the **Relation** column to select an action operation.

The following actions are available:

- ==
- !=
- <
- >
- <=
- >=
- contains
- matches

4. Define a filter by entering a value that corresponds to the selected property in the **Value** column.
5. Repeat steps 2 through 4 as needed to define more filters.
6. Click **OK**.

The **Port Connectivity View** dialog box displays. If filtering is already enabled, only those ports that meet the filter requirements display. To enable the filter, select the **Filter** check box.

### *Resetting the filter*

Reset immediately clears all existing definitions. You cannot cancel the reset.

To reset the **Filter** dialog box, complete the following steps.

1. Click the **Filter** link from the **Port Connectivity View** dialog box.

The **Filter** dialog box displays.

2. Click **Reset**.

All existing definitions are cleared automatically. You cannot cancel the reset.

### *Enabling the filter*

To enable the filter, select the **Filter** check box.

### *Disabling the filter*


To disable the filter, clear the **Filter** check box.

## Viewing port details

To view port details, complete the following steps.

1. Right-click the port for which you want to view more detailed information on the **Port Connectivity View** dialog box and select **Show Details**.

The **Port Details** dialog box displays (Figure 91).

COLUMN 	VALUE	
Actual Distance		
Area ID (Hex)/Port Index (Hex)	20	
Blade Number	N/A	
Blocked		
Buffer Limited	N/A	
Buffers Needed/Allocated		
COS		
Capability		
Connected Blade Number	N/A	
Connected Port Area ID (Hex)/Port Index (Hex)	0 (0x00)	
Connected Port Name		
Connected Port Number	0	
Connected Port Speed		
Connected Port State		
Connected Port Status		
Connected Port WWN		
Connected User Port Number (Hex)		
Device Node WWN		
Device Port / Switch Domain Id		
Device Port / Switch Manufacturer		
Device Port / Switch Manufacturing Plant		
Device Port / Switch Name		
Device Port / Switch State		
Device Port / Switch Type Number		
Device Port / Switch WWN		

**FIGURE 93** Port Details dialog box

2. Review the port information.

For the list of fields on the **Port Details** dialog box, refer to [Table 13](#) on page 213.

3. Sort the results by clicking on the column header.
4. Rearrange the columns by dragging and dropping the column header.
5. Click the close (X) button to close this dialog box.

## Viewing ports and port properties

To view ports on the Connectivity Map, right-click a product icon and select **Show Ports**.

**NOTE**

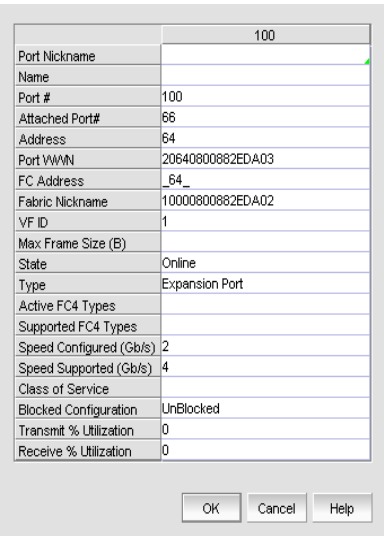
**Show Ports** is not applicable when the map display layout is set to **Free Form** (default).

**NOTE**

This feature is only available for connected products. On bridges and CNT products, only utilized Fibre Channel ports display; IP ports do not display.

To view a port's properties, right-click on a port and select **Properties**, or double-click on the port.

The port **Properties** dialog box displays (Figure 91).



	100
Port Nickname	
Name	
Port #	100
Attached Port#	66
Address	64
Port WWN	20640800882EDA03
FC Address	_64_
Fabric Nickname	10000800882EDA02
VF ID	1
Max Frame Size (B)	
State	Online
Type	Expansion Port
Active FC4 Types	
Supported FC4 Types	
Speed Configured (Gb/s)	2
Speed Supported (Gb/s)	4
Class of Service	
Blocked Configuration	UnBlocked
Transmit % Utilization	0
Receive % Utilization	0

OK Cancel Help

**FIGURE 94** Port Properties dialog box

The following port types are available depending on the selected device:

- FC Ports
- GigE Ports
- IP Ports
- iSCSI Ports

**NOTE**

iSCSI ports that have an FC Address of all zeros are inactive. All others are active.

- Virtual Sessions Ports
- Virtual FCoE Ports

Depending on the port type, some of the following properties ([Table 13](#)) may not be available for all products.

**TABLE 13** Port properties

Field	Description
# Virtual Session Ports	The number of virtual session ports associated with the GE port.
Additional Port Info	Additional error information relating to the selected port.
Address	The address of the port.
Active FC4 Types	The active FC4 types.
Active Tunnels	The number of active tunnels.
Area ID (hex)/Port Index (hex)	The area identifier, in hexadecimal, of the switch-to-product connection.
Associated GE Port	The port number of the associated GE port.
Attached Port #	The port number of the attached product.
Blocked	The configuration of the switch (blocked or unblocked).
Buffers Desired	The number of buffers desired but not allocated.
Buffers Allocated	The number of buffers allocated.
Class	The class of the port.
Class of Service	The class of service.
Connected Devices	The number of connected devices. Click the icon in the right side of the field to open the <b>Virtual FCoE Port &lt;Number&gt; Connected Devices</b> dialog box.
Connected Switch	The name of the connected switch.
Delete button	Click to delete.
Device Type	Whether the device is an initiator or target.
Distance Actual (km)	The actual distance (in km) for end-to-end port connectivity.
Distance Estimated (km)	The estimated distance (in km) for end-to-end port connectivity.
Fabric	The fabric's IP address.
Fabric Name	The name of the fabric.
FCIP Capable	Whether the port is FCIP capable.
FC Port Count	The number of FC ports on the device.
Flag (FICON related)	Whether a flag is on or off.
GigE Port Count	The number of GigE ports on the device.
Inband Management Status	The inband management status (online or offline).
Index	The index of the Virtual FCoE Port.
Interface Count	The interface count.
iSCSI button	Click to launch the Element Manager.
iSCSI Capable	Whether the port is iSCSI capable or not.
Locked Port Type	The port type of the locked product.
Long Distance Setting	Whether the connection is considered to be normal or longer distance.

**TABLE 13** Port properties (Continued)

Field	Description
<b>MAC Address</b>	The Media Access Control address assigned to a network adapters or network interface cards (NICs).
<b>Manufacturer Plant</b>	The name of the manufacturer plant.
<b>Modify</b> button	Click to launch the Element Manager.
<b>Model</b>	The model number of the device.
<b>Name</b>	The name of the switch.
<b>Performance</b> list	Select to launch the dialog box of one of the following performance options: <ul style="list-style-type: none"> <li>• Real Time Graph</li> <li>• Historical Graph</li> <li>• Historical Report</li> </ul>
<b>Physical/Logical</b>	Whether the port is a physical port or a logical port.
<b>Port Address</b>	The address of the port.
<b>Port #</b>	The number of the port.
<b>Port ID</b>	The identifier of the port.
<b>Port Module</b>	The port's module.
<b>Port NPIV</b>	Number of NPIV ports.
<b>Port Speed (Gb/s)</b>	The port speed, in Gbits per second.
<b>Port State</b>	The port state (online or offline).
<b>Port Status</b>	The port's operational status (online or offline).
<b>Port WWN</b>	The port's world wide name.
<b>Prohibited</b>	Whether the port is prohibited.
<b>Protocol</b>	The network protocol, for example, Fibre Channel.
<b>Serial #</b>	The hardware serial number.
<b>Slot #</b>	The location (slot) of the port.
<b>Speed (Gb/s)</b>	The port speed, in Gbits per second.
<b>State</b>	The port state (online or offline).
<b>Status</b>	The port's operational status (online or offline).
<b>Switch</b>	The name of the switch.
<b>Symbolic Name</b>	The symbolic name of the port.
<b>Tag</b>	The tag number of the port.
<b>Troubleshooting</b> list	Select to launch the dialog box of one of the following troubleshooting options: <ul style="list-style-type: none"> <li>• IP Ping</li> <li>• IP Traceroute</li> <li>• IP Performance</li> </ul>
<b>Type</b>	The type of port, for example, U_port.
<b>Tunnel Count</b>	The number of tunnels.
<b>User Port #</b>	The number of the user port.

**TABLE 13** Port properties (Continued)

Field	Description
Vendor	The product vendor.
Virtual FCoE Port Count	The number of FC ports on the device.

## Port types

On the Connectivity Map, right-click a switch icon and select **Show Ports**. The port types display showing which ports are connected to which products.

### NOTE

**Show Ports** is not applicable when the map display layout is set to **Free Form** (default).

### NOTE

This feature is only available for connected products. On bridges and CNT products, only utilized Fibre Channel ports display. IP ports do not display.

**TABLE 14** Port types

Port Type	Description
E	An expansion port connecting two Fibre Channel switches.
EX	On a Fibre Channel Router, a connection between a fibre channel router and a fibre channel switch
F	On a Fibre Channel switch, a port that supports an N_Port.
FL	An N_port or F_port that supports arbitrated loop functions associated with arbitrated loop topology.
VE	A virtual E_port configured for an FCIP Tunnel.
VEX	A virtual EX_port configured in an FCIP Tunnel.

## Showing connected ports

You can jump from a port to its connected port.

1. Right-click the product whose port connection you want to determine and select **Show Ports**.  
The product's ports display.
2. Right-click a port and select **Connected Port**.  
The focus jumps to the connected port and the connection is highlighted.

## Viewing port connection properties

You can view the information about products and ports on both sides of the connection.

1. Right-click the connection between two end devices on the Connectivity Map and select **Properties**.

OR

Double-click the connection between two devices on the Connectivity Map.

The **Connection Properties** dialog box displays.

### NOTE

If one of the devices is in an unknown state, the Product 1 and Product 2 information displays; however, the **Connections** table information does not display.

2. Review the following information:
  - Product properties for both devices.
  - Connection properties.
  - Selected connection port properties.

Depending on the device type at either end of the connection, some of the following fields (Table 15) may not be available for all products.

**TABLE 15** Port connection properties

Field	Description
<b>Product Properties</b> table	The product information for the two connected switches.
<b>Domain ID</b>	The domain ID of the selected switch and product in xxs(yy) format, where xx is the normalized value and yy is the actual value.
<b>Fabric Name</b>	The world wide name of the fabric.
<b>IP Address</b>	The IP address of the switch.
<b>Switch Name</b>	The name of the switch.
<b>WWN</b>	The world wide name of the switch.
<b>Connections</b> table	One row for each circuit.
<b>1-Port #</b>	The port number of the first switch.
<b>1-Port Type</b>	The port type of the first switch.
<b>1-WWPN</b>	The world wide port number of the first switch.
<b>1-MAC Address</b>	The media access control (MAC) address of the first switch.
<b>1-IP Address</b>	The IP address of the first switch.
<b>1-Trunk</b>	Whether there is a trunk on the first switch.
<b>1-Speed (Gbps)</b>	The speed of the first switch.
<b>2-Port #</b>	The port number of the second switch.
<b>2-Port Type</b>	The port type of the second switch.
<b>2-WWPN</b>	The world wide port number of the second switch.
<b>2-MAC Address</b>	The MAC address of the second switch.

**TABLE 15** Port connection properties (Continued)

Field	Description
2-IP Address	The IP address of the second switch.
2-Trunk	Whether there is a trunk on the second switch.
2-Speed (Gbps)	The speed of the second switch.
Selected Connection Properties table	The connected device port information.
Area ID (hex)/Port Index (hex)	The area identifier, in hexadecimal, of the switch-to-product connection.
Blocked	The configuration of the switch (blocked or unblocked).
Buffers Allocated	The number of buffers allocated.
Buffers Desired	The number of buffers required but not allocated.
Circuits	The circuit number of the connected switch.
Connected Switch	The name of the connected switch.
Cost	The cost of the ISL link.
Distance Actual (km)	The actual distance (in km) for end-to-end port connectivity.
Distance Estimated (km)	The estimated distance (in km) for end-to-end port connectivity.
ED TOV	The Error Detect timeout value, in milliseconds, of the connected switch. This variable is used to flag a potential error condition when an unexpected response is not received.
FC Address	The Fibre Channel (FC) address of the switch.
FC Port #	The FC port number of the switch.
Flag (FICON related)	Whether a FICON-related flag is on or off.
GE Port #	The GE port number of the switch.
Locked Port Type	The port type of the locked product.
Long Distance Setting	Whether the connection is considered to be normal or longer distance.
MAC Address	The MAC address of the switch.
Manufacturer	The name of the manufacturer.
Manufacturer Plant	The name of the manufacturing plant.
Name	The name of the switch.
NPIV Enabled	Whether the NPIV port is enabled.
Parameter	The parameter of the switch.
Physical/Logical	Whether the port is a physical port or a logical port.
PID Format	The port ID format of the switch.
Port Address	The address of the port.
Port Module	The port's module.
Port NPIV	The number of NPIV ports.
Port Type	The type of port.
Prohibited	Whether the port is prohibited.

**TABLE 15** Port connection properties (Continued)

Field	Description
Protocol	The network protocol, for example, Fibre Channel.
RA TOV	The resource allocation time out value, in milliseconds, of the connected switch. This variable works with the E D TOV variable to determine switch actions when presented with an error condition.
Sequence #	The sequence number of the switch.
Serial #	The serial number of the switch.
Slot #	The slot number of the switch.
Speed (Gb/s)	The speed in gigabytes per second.
State	The operational status of the port.
Status	The operational status of the switch
Tag	The tag number of the switch.
Trunking Enabled	Whether trunking is enabled on the switch.
Tunnel ID	The tunnel ID number of the switch.
User Port #	The user port number of the switch.

3. Click **Close** to close the dialog box.

## Determining inactive iSCSI devices

For router-discovered iSCSI devices, you can view all of the inactive iSCSI devices in one list. To do this, use the **Ports Only** view and then sort the devices by FC Address. The devices that have an FC address of all zeros are inactive.

1. Select **View All, Levels**, and then **Ports Only** from the main window.
2. Use the scroll bar to view the columns to the right and locate the **FC Address** column in the **Ports Only** list.
3. Click the column label to sort the column in ascending order, if needed.

iSCSI ports that have an FC Address of all zeros are inactive. All others are active.

## Determining port status

You can determine whether a port is online or offline by looking at the Connectivity Map or the Product List. On the Connectivity Map, right-click on the product whose ports you want to view and select **Show Ports**.

To determine a port's status through the Product List, scroll down the Product List to the product whose ports you want to see and click the added icon (+).

## Viewing port optics

To view port optics, complete the following steps.

1. Right-click the switch for which you want to view port optic information on the Connectivity Map and select **Port Optics (SFP)**.

The **Port Optics (SFP)** dialog box displays (Figure 95).

FC Address	TX Power	RX Power	Xceiver Temp	Vendor	Vendor OUI
940f00	0.0	306.5	46	AGILENT	00:30:d3
940000	0.0	338.5	41	AGILENT	00:30:d3
940d00	0.0	241.5	49	FINISAR CORP.	00:90:65
940400	0.0	0.0	45	AGILENT	00:30:d3
940a00	0.0	300.299988	47	AGILENT	00:30:d3

**FIGURE 95** Port Optics dialog box

2. Review the port optics information.
  - **Slot/Port #**—The slot and port number of the selected fabric.
  - **FC Address**—The Fibre Channel address of the port.
  - **TX Power**—The power transmitted to the SFP in dBm and uWatts.

---

### NOTE

The uWatts display requires devices with Fabric OS 6.1.0 and later. Devices running Fabric OS 6.0.0 and earlier only display dBm.

---

- **RX Power**—The power received from the port in dBm and uWatts.

---

### NOTE

The uWatts display requires devices with Fabric OS 6.1.0 and later. Devices running Fabric OS 6.0.0 and earlier only display dBm.

---

- **Transceiver Temp**—The temperature of the SFP transceiver.
- **Vendor**—The vendor of the SFP.
- **Vendor OUI**—The vendor's organizational unique identifier (OUI).
- **FC Speed**—The FC port speed; for example, 400 Mbps.
- **Distance**—The length of the fiber optic cable.

- **Vendor PN**—The part number of the SFP.
  - **Vendor Rev**—The revision number of the SFP.
  - **Serial #**—The serial number of the SFP.
  - **Data Code**—The data code.
  - **Media Form Factor**—The type of media for the transceiver; for example, single mode.
  - **Connector**—The type of port connector.
  - **Wave Length**—The wave length.
  - **Encoding**—Displays how the fiber optic cable is encoded.
  - **Voltage (mVolts)**—The voltage across the port in mVolts.
3. Sort the results by clicking on the column header.
  4. Rearrange the columns by dragging and dropping the column header.
  5. Click **Cancel** to close the **Port Optics (SFP)** dialog box.

### *Refreshing port optics*

To refresh port optics, click **Refresh**.

The Management application retrieves updated port optic information.

## Port Auto Disable

The **Port Auto Disable** dialog box allows you to enable and disable the port auto disable flag on individual FC\_ports or on all ports on a selected device, as well as unblock currently blocked ports.

### NOTE

The device must be running Fabric OS 6.3 or later.

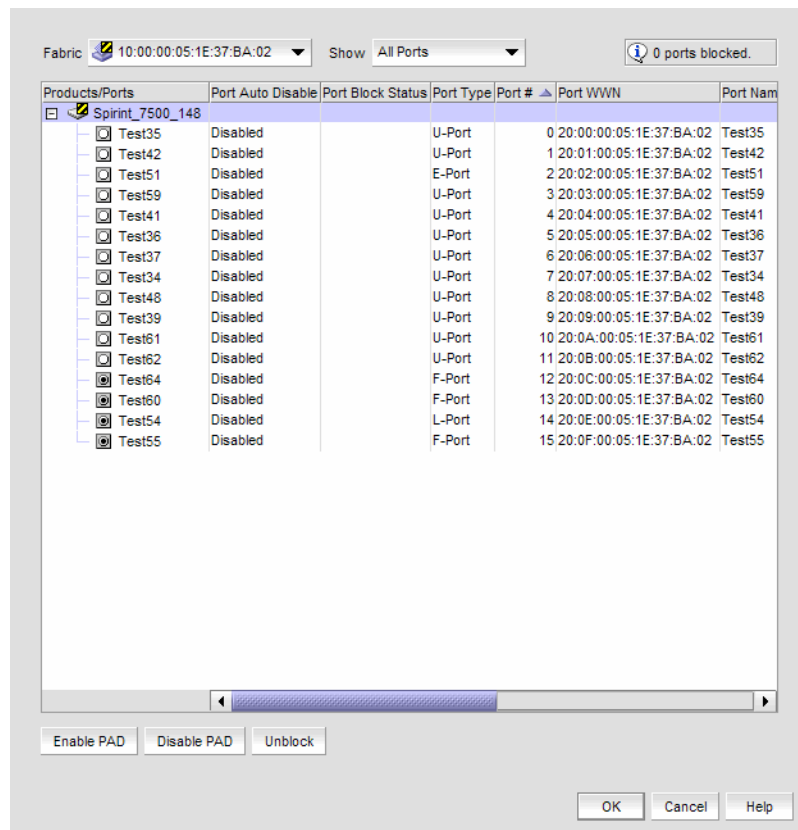
## Viewing the port auto disable status

### NOTE

The device must be running Fabric OS 6.3 or later.

1. Select **Configure > Port Auto Disable**.

The **Port Auto Disable** dialog box displays.



**FIGURE 96** Port Auto Disable dialog box

2. Review the port status and other information:
  - **Products/Ports** tree—Displays devices and associated ports. Also, displays a Warning icon for blocked FC ports (displayed with the port icon).
  - **Port Auto Disable**—Displays whether Port Auto Disable is currently enabled or disabled.
  - **Port Block Status**—Displays whether the port is currently blocked.

- **Port Type**—Displays the port type.
- **Port Number**—Displays the port number.
- **Port WWN**—Displays the port world wide name.
- **Port Name**—Displays the port name.
- **User Port #**—Displays the user port number.
- **PID**—Displays the port identifier.
- **Connected Port #**—Displays the connected port number.
- **Connected Port WWN**—Displays the connected port world wide name.
- **Connected Port Name**—Displays the connected port name.

3. Click **OK** on the **Port Auto Disable** dialog box.

### Enabling port auto disable on individual ports

---

**NOTE**

The device must be running Fabric OS 6.3 or later.

---

1. Select **Configure > Port Auto Disable**.  
The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Choose one of the following options from the **Show** list to filter the port list:
  - **All Ports** (default)—Displays all ports in the fabric.
  - **Disabled PAD**—Displays only ports where PAD is enabled.
4. Select the ports on which you want to enable PAD.
5. Click **Enable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

### Enabling port auto disable on all ports on a device

---

**NOTE**

The device must be running Fabric OS 6.3 or later.

---

1. Select **Configure > Port Auto Disable**.  
The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Select **All Ports** from the **Show** list.
4. Select the device on which you want to enable PAD on all ports.
5. Click **Enable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

## Disabling port auto disable on individual ports

---

**NOTE**

The device must be running Fabric OS 6.3 or later.

---

1. Select **Configure > Port Auto Disable**.  
The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to disable port auto disable (PAD) from the **Fabric** list.
3. Choose one of the following options from the **Show** list to filter the port list:
  - **All Ports** (default)—Displays all ports in the fabric.
  - **Enabled PAD**—Displays only ports where PAD is enabled.
4. Select the ports on which you want to disable PAD.
5. Click **Disable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

## Disabling port auto disable on all ports on a device

---

**NOTE**

The device must be running Fabric OS 6.3 or later.

---

1. Select **Configure > Port Auto Disable**.  
The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to disable port auto disable (PAD) from the **Fabric** list.
3. Select **All Ports** from the **Show** list.
4. Select the device on which you want to disable PAD on all ports.
5. Click **Disable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

## Unblocking ports

---

**NOTE**

The device must be running Fabric OS 6.3 or later.

---

1. Select **Configure > Port Auto Disable**.  
The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Select **Blocked Ports** from the **Show** list.
4. Select the device on which you want to enable PAD on all ports.
5. Click **Enable PAD**.
6. Click **OK** on the **Port Auto Disable** dialog box.

## Storage port mapping configuration

The Management application enables you to see multiple ports on your storage devices in a SAN. It also displays the relationship between multiple ports and represents them as attached to a storage array (device) in the **Device Tree**, **Topology**, and **Fabric** views. Occasionally, there are cases where the Management application cannot see the relationship between ports attached to the same storage device. Therefore, the Management application allows you to manually associate the connections that the system is unable to make.

The Management application allows you to create and assign properties to a Storage Device during the mapping process using the **Storage Port Mapping** dialog box. Once a Storage Device has multiple ports assigned to it you cannot change the device type.

---

### NOTE

When you open the **Storage Port Mapping** dialog box, Discovery is automatically turned off. When you close the **Storage Port Mapping** dialog box, Discovery automatically restarts.

---

During Discovery, if a previously mapped Storage Port is found to have a relationship with a port just discovered, the Management application automatically reassigns the Storage Port to the proper mapping. The two Ports are grouped together. This grouping is visually represented as a Storage Device. This Storage Device contains Node information from the discovered port and populates default information where available.

The Management application allows you to change the Device Type of a discovered device. Isolated Storage Ports are represented as Storage Devices. Using the Storage Port Mapping dialog you cannot change the device type to an HBA, JBOD, and so on. However, once a device has been identified as type Storage with ports assigned, you can no longer change its type.

## Creating a storage array

To create a storage array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.

2. Click **New Storage**.

A new storage array displays in the **Storage Array** list in edit mode.

3. Rename the new storage array and press **Enter**.
4. Add storage ports to the new storage array.

---

### NOTE

You must add at least one storage ports to the new storage array to save the new array in the system.

---

For step-by-step instructions about adding ports to an array, refer to [“Adding storage ports to a storage array”](#) on page 225.

5. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

## Adding storage ports to a storage array

To add storage ports to a storage array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.The **Storage Port Mapping** dialog box displays.
2. Select a storage port from the **Storage Ports** table.

To select more than one port, hold down the **CTRL** key while selecting multiple storage ports.
3. Select the storage array to which you want to assign the storage port in the **Storage Array** list.
4. Click the right arrow.

The storage port is added to the Storage Array.
5. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

## Unassigning a storage port from a storage array

To unassign a storage port from a storage array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.The **Storage Port Mapping** dialog box displays.
2. Select the storage port you want to unassign from the **Storage Array** list.
3. Click the left arrow button.

The selected storage port is removed from the **Storage Array** list and added to the **Storage Ports** table.
4. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

## Reassigning mapped storage ports

To reassign a storage port, complete the following steps.

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.The **Storage Port Mapping** dialog box displays.

2. Select the storage port you want to unassign from the **Storage Array** list.
3. Click the left arrow button.

The selected storage port is removed from the **Storage Array** list and added to the **Storage Ports** table.
4. Make sure the storage port you want to reassign is still selected.
5. Select the storage array to which you want to reassign the storage port in the **Storage Array** list.
6. Click the right arrow button.

The storage port moves from the **Storage Ports** table to the selected storage array.
7. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

### Editing storage array properties

To edit storage array properties, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.
2. Select the storage array in the **Storage Array** list and click **Properties**.

The **Properties** dialog box appears.
3. Edit the property fields, as needed.

Depending on which tab you select (Properties tab, Storage tab, Port tab), different fields will be available for editing. Editable fields have a green triangle in the lower right corner of the field.
4. Click **OK** on the **Properties** dialog box to save the storage array properties.
5. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

### Deleting a storage array

To delete a storage array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.
2. Select a storage array in the **Storage Array** list.

3. Click **Delete**.

The selected storage array and all storage ports assigned to the array are removed from **Storage Array** list. All Storage Ports assigned to the device are moved to the **Storage Ports** table.

4. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

## Viewing storage port properties

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.

2. Select a storage port from the **Storage Array** list.
3. Click **Properties**.

The **Properties** dialog box displays.
4. Review the properties.
5. Click **OK** on the **Properties** dialog box.
6. Click **OK** on the **Storage Port Mapping** dialog box.

## Viewing storage array properties

To view storage array properties, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.

2. Select a storage array from the **Storage Array** list.
3. Click **Properties**.

The **Properties** dialog box displays.
4. Review the properties.
5. Click **OK** on the **Properties** dialog box.
6. Click **OK** on the **Storage Port Mapping** dialog box.

## Importing storage port mapping

The **Storage Port Mapping** dialog box enables you to import externally created storage port mapping information into the application. The imported file must be in CSV format. The first row must contain the headers (wwn, name) for the file, which is ignored during the import.

### Example

```
wwn,name
20:00:00:04:CF:BD:89:6E,name1
20:00:00:04:CF:BD:6F:32,name2
20:00:00:04:CF:BD:70:2F,name1
20:00:00:04:CF:BD:6F:52,name2
```

To import storage port mapping, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.

2. Click **Import**.

The **Import** dialog box displays.

3. Browse to the file (CSV format only) you want to import.
4. Click **Open** on the **Import** dialog box.

The file imports, reads, and applies all changes line-by-line and performs the following:

- Checks for correct file structure (first entry must be the storage node name (WWN) and second entry must be the storage array name), well formed WWNs, and counts number of errors  
If more than 5 errors occur, import automatically cancels. Edit the storage port mapping file and try again.
- Checks for duplicate storage ports (the same storage port mapped to more than one storage array)  
If duplicates exist, a message displays with the duplicate mappings detailed. Click **Yes** to continue. Click **No** to edit the storage port mapping file and try again.
- Checks if mapping exists in current map  
If mappings already exist, a message displays with the current mapping information. Click **Yes** to overwrite the current mapping. Click **Yes to All** to overwrite all mapping conflicts. Click **No** to leave the current mapping. Click **No to All** to leave all current mappings when conflict occurs. Click **Cancel** to cancel the import.

When import is complete a result summary displays with the following information (“[Import Results](#)” on page 229).

**TABLE 16** Import Results

Value	Definition
<b>Total Valid Input Records</b>	Number of lines identified in the CSV file without any errors (excluding the Header).
<b>Unique storage port WWN's Recognized</b>	Number of unique storage ports identified in the CSV file.
<b>Storage Arrays Created or Identified</b>	Number of storage ports identified in the CSV file already discovered and are either online or offline but not deleted.
<b>Conflicting Port Mappings</b>	Number of occurrences where you were asked to decide whether to override previously discovered information. If a you select Yes to All, or No to All, each occurrence where conflict resolution occurs automatically is counted as one conflict.
<b>Overwritten Port Mappings</b>	Number of times a previously discovered mapping is overwritten during the import process.
<b>Importing Errors</b>	Number of errors encountered during the import.
<b>Details</b>	Tabulates the error information with respect to the line number where it occurred.

5. Click **OK** to close the **Import Results** dialog box.
6. Click **OK** to close the **Storage Port Mapping** dialog box.

## Exporting storage port mapping

The **Storage Port Mapping** dialog box enables you to export a storage port array. The export file uses the CSV format. The first row contains the headers (Storage Node Name (WWNN), Storage Array Name) for the file.

### Example

```
Storage Node Name (WWNN), Storage Array Name
20000004CFBD7100,New Storage Array
20000004CFBD896E,New Storage Array
2000002037E19CED,New Storage Array
```

To export a storage port array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
    - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
    - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
    - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.
  2. Select the storage port array you want to export port from the **Storage Array** list.
  3. Click **Export**.
- The **Export** dialog box displays.

4. Browse to the location where you want to save the export file.  
Depending on your operating system, the default export location are as follows:
  - Desktop\My documents (Windows)
  - \root (Linux)
  - \ (Solaris)
5. Enter a name for the files and click **Save**.
6. Click **OK** to close the **Storage Port Mapping** dialog box.

## Device Technical Support

You can use Technical Support to collect supportSave data (such as, RASLOG, TRACE and so on) and switch events from Fabric OS devices. You can gather technical data for M-EOS devices using the device's Element Manager.

To gather technical support information for the Management application server, refer to [“Capturing technical support information”](#) on page 167.

### Scheduling technical support information collection

---

#### NOTE

The switch must be running Fabric OS 5.2.X or later to collect technical support data.

---



---

#### NOTE

You must have the SupportSave privilege to perform this task.

---

To capture technical support and event information for specified devices, complete the following steps.

1. Select **Monitor > Technical Support > Switch/Host SupportSave**.  
The **Technical SupportSave** dialog box displays.
2. Click the **Schedule** tab.
3. Select the **Enable scheduled Technical Support Data** check box.
4. Select how often you want the scheduled collection to occur from the **Frequency** list.
5. Select the start date for the scheduled collection from the **Start Date** list.  
This list is only available when you select Weekly or Monthly from the **Frequency** list.
6. Select the time you want the scheduled collection to begin from the **Start Time Hour** and **Minute** lists.
7. Right-click in the **Available Switches** table and select **Expand All**.
8. Select the switches you want to collect data for in the **Available Switches** table and click the right arrow to move them to the **Selected Switches** table.
9. Select how often you want to purge the support data from the **Purge Support Data** list.

10. Click **OK** on the **Technical SupportSave** dialog box.

11. Click **OK** on the confirmation message.

Technical supportSave data is saved to the following directory:

*Install\_Home\data\ftproot\technicalsupport\*

Technical supportSave uses the following naming convention for the files:

*Supportinfo-Day-mm-dd-yyyy-hh-mm-ss\Switch\_Type-Switch\_IP\_Address-Switch\_WWN.*

Data collection may take 20-30 minutes for each selected switch. This estimate may increase depending on the number of switches selected. Check the Master Log for status information.

## Starting immediate technical support information collection

---

### NOTE

The switch must be running Fabric OS 5.2.X or later to collect technical support data.

---



---

### NOTE

The HBA must be a managed Brocade HBA.

---



---

### NOTE

You must have the SupportSave privilege to perform this task.

---

To capture technical support and event information for specified devices, complete the following steps.

1. Select **Monitor > Technical Support > Switch/Host SupportSave**.

The **Technical SupportSave** dialog box displays.

2. Click the **Generate Now** tab, if necessary.

3. Click the **Switches** tab, if necessary, and complete the following steps.

a. Right-click in the **Available Switches** table and select **Expand All**.

b. Select the switches you want to collect data for in the **Available Switches** table and click the right arrow to move them to the **Selected Switches and Hosts** table.

4. Click the **Hosts** tab, if necessary, and complete the following steps.

a. Right-click in the **Available Hosts** table and select **Expand All**.

b. Select the switches you want to collect data for in the **Available Switches** table and click the right arrow to move them to the **Selected Switches and Hosts** table.

5. Click **OK** on the **Technical SupportSave** dialog box.

6. Click **OK** on the confirmation message.

Technical supportSave data is saved to the following directory:

*Install\_Home\data\ftproot\technicalsupport\*

Technical supportSave uses the following naming convention for the files:

*Supportinfo-Day-mm-dd-yyyy-hh-mm-ss\Switch\_Type-Switch\_IP\_Address-Switch\_WWN.*

Data collection may take 20-30 minutes for each selected switch. This estimate may increase depending on the number of switches selected. Check the Master Log for status information.

### Viewing technical support information

To view technical support information, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

The **Repository** dialog box displays.

2. Choose from one of the following options:

- Select the **Switches** tab to view technical support information on switches.
- Select the **Hosts** tab to view technical support information on Hosts.

3. Click **View** to view the repository in an Internet browser window.

The technical support information displays in an Internet browser window.

4. Click the appropriate link to view details.
5. Click **OK** on the **Repository** dialog box.

### E-mailing technical support information

To e-mail technical support information, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

The **Repository** dialog box displays.

2. Choose from one of the following options:

- Select the **Switches** tab to e-mail technical support information on switches.
- Select the **Hosts** tab to e-mail technical support information on Hosts.

3. Select the file you want to e-mail in the table.

4. Click **E-mail** to e-mail the switch event and supportsave files (zip).

You must configure the Management application e-mail server before you can define the e-mail action. For more information, refer to [“Configuring e-mail notification”](#) on page 274.

The **E-mail** dialog box displays.

5. Enter the e-mail address of the person to receive the e-mail in the **To** field.
6. Enter your e-mail address in the **From** field.
7. Click **OK**.

The e-mail is sent and the **Repository** dialog box closes automatically.

## Copying technical support information to an external FTP server

To copy the Support Save data located in the built-in FTP server to an external FTP server, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

The **Repository** dialog box displays.

2. Choose from one of the following options:

- Select the **Switches** tab to copy technical support information on switches.
- Select the **Hosts** tab to copy technical support information on Hosts.

3. Select the file you want to copy in the table.

4. Click **FTP** to send the switch event and supportsave files (zip) by FTP.

The **FTP Credentials** dialog box displays.

5. Enter the network address or domain name of the external FTP server in the **Network Address** field.
6. Enter your user name and password.
7. Enter the root directory where you want to copy the data on the external FTP server in the **Root Directory** field.
8. Click **OK**.

The data is copied and the **Repository** dialog box closes automatically.

## Deleting technical support files from the repository

To delete a technical support file from the repository, complete the following steps.

1. Select **Monitor > Technical Support > View Repository**.

The **Repository** dialog box displays.

2. Choose from one of the following options:

- Select the **Switches** tab to delete technical support information on switches.
- Select the **Hosts** tab to delete technical support information on Hosts.

3. Select the file you want to delete in the table.

4. Click **Delete**.

5. Click **OK** on the **Technical SupportSave** dialog box.

6. Click **OK** on the confirmation message.

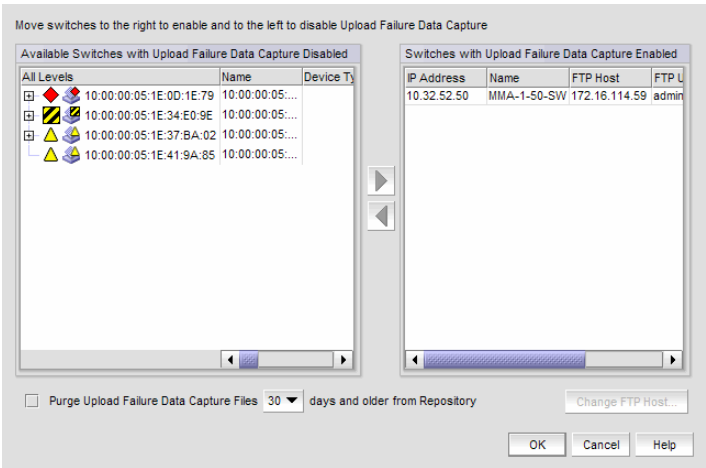
# Upload Failure data capture

You can use Upload Failure Data Capture to enable, disable, and purge failure data capture files as well as configure the FTP Host for the switch.

**NOTE**  
Upload Failure Data Capture is only supported on Fabric OS devices.

## Enabling upload failure data capture

- 1. Select **Monitor > Technical Support > Upload Failure Data Capture**.  
The **Upload Failure Data Capture** dialog box displays.



**FIGURE 97** Upload Failure Data Capture dialog box

- 2. Select a one or more devices on which you want to enable automatic trace dump from the **Available Switches with Upload Failure Data Capture Disabled** table.
- 3. Click the right arrow button.  
The selected devices move from the **Available Switches with Upload Failure Data Capture Disabled** table to the **Switches with Upload Failure Data Capture Enabled** table.
- 4. Click **OK** on the **Upload Failure Data Capture** dialog box.
- 5. Click **OK** on the confirmation message, if necessary.

## Disabling upload failure data capture

---

**NOTE**

Upload Failure Data Capture is only supported on Fabric OS devices.

---

1. Select **Monitor > Technical Support > Upload Failure Data Capture**.  
The **Upload Failure Data Capture** dialog box displays.
2. Select one or more devices on which you want to disable automatic trace dump from the **Available Switches with Upload Failure Data Capture Enabled** table.
3. Click the left arrow button.  
The selected devices move from the **Switches with Upload Failure Data Capture Enabled** table to the **Available Switches with Upload Failure Data Capture Disabled** table.
4. Click **OK** on the **Upload Failure Data Capture** dialog box.
5. Click **OK** on the confirmation message, if necessary.

## Purging upload failure data capture files

---

**NOTE**

Upload Failure Data Capture is only supported on Fabric OS devices.

---

1. Select **Monitor > Technical Support > Upload Failure Data Capture**.  
The **Upload Failure Data Capture** dialog box displays.
2. Select the **Purge Upload Failure Data Capture Files** check box to enable purging the trace dump files.
3. Select how often (days) you want to purge the trace dump data from the **Purge Upload Failure Data Capture Files** list.
4. Click **OK** on the **Upload Failure Data Capture** dialog box.

## Configuring the upload failure data capture FTP server

### NOTE

Upload Failure Data Capture is only supported on Fabric OS devices.

### NOTE

Some external FTP software (such as, Filezilla and Xlight) are not supported.

1. Select **Monitor > Technical Support > Upload Failure Data Capture**.

The **Upload Failure Data Capture** dialog box displays.

2. Select a device from the **Available Switches with Upload Failure Data Capture Enabled** table.
3. Click **Change FTP Host**.

The **Change FTP Server** dialog box displays.

**FIGURE 98** Change FTP Server dialog box

4. Choose one of the following options:
  - Select the **Use Management\_Application** option to use the Management application FTP server.
  - Select the **Custom** option and complete the following steps to configure a FTP server for the selected device.
    - a. Enter the server's IP address in the **Host IP** field.
    - c. Enter a user name for the server in the **User Name** field.
    - d. Enter a password for the server in the **Password** field.
    - e. Enter the path to where the trace dump data is saved in the **Directory Path** field.
5. Click **Test** to test the server credentials.
6. Click **OK** on the **Change FTP Host** dialog box.
7. Click **OK** on the **Upload Failure Data Capture** dialog box.
8. Click **OK** on the confirmation message, if necessary.

## Viewing the upload failure data capture repository

---

**NOTE**

Upload Failure Data Capture is only supported on Fabric OS devices.

---

1. Select **Monitor > Technical Support > View Repository**.  
The **Repository** dialog box displays.
2. Select the trace dump file you want to view from the **Available Support and Upload Failure Data Capture Files** table.
3. Click **View**.  
The Upload Failure Data Capture repository displays.

## 8 Viewing the upload failure data capture repository

# Fabric Binding

---

## In this chapter

- [Fabric binding overview](#) . . . . . 239
- [Enabling fabric binding](#) . . . . . 240
- [Disabling fabric binding](#) . . . . . 241
- [Adding switches to the fabric binding membership list](#) . . . . . 241
- [Adding detached devices to the fabric binding membership list](#) . . . . . 242
- [Removing switches from fabric binding membership](#) . . . . . 242
- [High integrity fabrics](#) . . . . . 243

## Fabric binding overview

---

### NOTE

In a pure Fabric OS environment, Fabric Binding is supported on Fabric OS 5.2 or later.

---



---

### NOTE

In a mixed Fabric OS and M-EOS environment, Fabric Binding in Interop Mode 2 or 3 is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

---



---

### NOTE

To enable or disable Fabric Binding in a mixed fabric, at least one Fabric OS device and one M-EOS device must be manageable.

---



---

### NOTE

In a mixed Fabric OS and M-EOS environment, you cannot disable Fabric Binding if High Integrity Fabric is enabled. However, if High Integrity Fabric is disabled, you can disable Fabric Binding.

---

The fabric binding feature enables you to configure whether switches can merge with a selected fabric. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

For M-EOS devices, enabling Fabric Binding activates Fabric Binding and enables insistent domain ID. Disabling Fabric Binding on M-EOS devices deactivates Fabric Binding.

For Fabric OS devices, enabling Fabric Binding activates Switch Connection Control (SCC) policy and sets Fabric Wide Consistency Policy (FWCP) and insistent domain ID. Disabling Fabric Binding on Fabric OS devices deletes SCC policy and sets FWCP to absent.

---

### NOTE

In a pure Fabric OS fabric, enabling insistent domain ID is mandatory.

---

## Enabling fabric binding

Fabric Binding is enabled through the **Fabric Binding** dialog box. After you have enabled Fabric Binding, use the **Fabric Membership List/Add Detached Switch** to add switches that you want to allow into the fabric.

### NOTE

In a pure Fabric OS environment, Fabric Binding is only supported on Fabric OS 5.2 or later. In a mixed Fabric OS and M-EOS environment, Fabric Binding is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

1. Select **Configure > Fabric Binding**.

The **Fabric Binding** dialog box displays (Figure 99).

**Fabric List**

Fabric Name	Fabric WWN	Binding Status	Enable/Disable	Action
10:00:00:05:1E:34:E0:9E	10:00:00:05:1E:34:...	Enabled	<input checked="" type="checkbox"/>	
10:00:00:05:1E:37:BA:02	10:00:00:05:1E:34:...	Disabled	<input type="checkbox"/>	
10:00:00:05:1E:41:9A:85	10:00:00:05:1E:41:...	Enabled	<input checked="" type="checkbox"/>	

**Available Switches**

Name	Node WWN	Domain ID	Fabric Name	Fabric V
dcfm_sprint148	10:00:00:05:...	148 (52)	10:00:00:05:...	10:00:00:05:...
efcm_pulsar_108	10:00:00:05:...	108 (12)	10:00:00:05:...	10:00:00:05:...
efcm_pulsar_115	10:00:00:05:...	115 (19)	10:00:00:05:...	10:00:00:05:...
MMA-1-50-SW	10:00:00:05:...	4	10:00:00:05:...	10:00:00:05:...

**Membership List of 10:00:00:05:1E:41:9A:85**

Name	Node WWN	Domain ID	Fabric Name	Fabric V
MMA-1-50-SW	10:00:00:05:...	4	10:00:00:05:...	10:00:00:05:...

Add Detached Switch...

OK Cancel Help

**FIGURE 99** Fabric Binding dialog box

2. In the **Fabric List** table, click the **Enable/Disable** check box for fabrics for which you want to configure fabric binding.

For instructions on adding and removing switches from the membership list, refer to [“Adding switches to the fabric binding membership list”](#) on page 241 and [“Removing switches from fabric binding membership”](#) on page 242.

3. Click **OK**.

## Disabling fabric binding

Fabric Binding cannot be disabled while High Integrity Fabric is active if the switch is offline. This disables fabric binding and High Integrity Fabric on the switch, but not the rest of the fabric. Disabled switches segment from the fabric. Fabric Binding is disabled through the **Fabric Binding** dialog box.

---

### NOTE

In a pure Fabric OS environment, Fabric Binding is only supported on Fabric OS 5.2 or later. In a mixed Fabric OS and M-EOS environment, Fabric Binding is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

---

1. Select **Configure > Fabric Binding**.

The **Fabric Binding** dialog box displays.

2. In the **Fabric List** table, clear the **Enable/Disable** check box for fabrics for which you want to disable fabric binding.
3. Click **OK**.

## Adding switches to the fabric binding membership list

Once you have enabled Fabric Binding (refer to [“Enabling fabric binding”](#) on page 240), you can add switches to the fabric binding membership list.

---

### NOTE

In a pure Fabric OS environment, Fabric Binding is only supported on Fabric OS 5.2 or later. In a mixed Fabric OS and M-EOS environment, Fabric Binding is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

---

To add a switch to the fabric, complete the following steps.

1. Select **Configure > Fabric Binding**.

The **Fabric Binding** dialog box ([Figure 99](#)) displays.

2. Select the switches you want to add to the selected fabrics' Fabric Membership List (FML) in the **Available Switches** table.
3. Click the right arrow to move the switches to the **Membership List** table.
4. Click **OK** on the **Fabric Binding** dialog box.

## Adding detached devices to the fabric binding membership list

To add a switch that does not have a physical connection and is not discovered to the fabric, complete the following steps.

1. Select **Configure > Fabric Binding**.  
The **Fabric Binding** dialog box displays.
2. Click **Add Detached Switch**.  
The **Add Detached Switch** dialog box displays.
3. Enter the domain ID of the switch in the **Domain ID** field.
4. Enter the node WWN of the switch in the **Node WWN** field.
5. Click **OK** on the **Add Detached Switch** dialog box.  
The added switch displays in the **Membership List of Fabric\_Name** table on the **Fabric Binding** dialog box.
6. Click **OK** on the **Fabric Binding** dialog box.

## Removing switches from fabric binding membership

Once you have enabled Fabric Binding (refer to [“Enabling fabric binding”](#) on page 240), you can remove switches that are not part of the fabric from the membership list.

---

### NOTE

In a pure Fabric OS environment, Fabric Binding is only supported on Fabric OS 5.2 or later. In a mixed Fabric OS and M-EOS environment, Fabric Binding is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

---

1. Select **Configure > Fabric Binding**.  
The **Fabric Binding** dialog box ([Figure 99](#)) displays.
2. Select the switches you want to remove from the selected fabrics' Fabric Membership List (FML) in the **Membership List** table.

---

### NOTE

The selected switch cannot be part of the fabric.

---

3. Click the left arrow to move the switches to the **Available Switches** table.
4. Click **OK**.

## High integrity fabrics

The High Integrity Fabric (HIF) mode option automatically enables features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. When HIF is enabled, each switch in the fabric automatically enforces a number of security-related features including Fabric Binding, Switch Binding, Insistent Domain IDs, and Domain Register for State Change Notifications (RSCNs).

For Pure Fabric OS fabrics, HIF activates the Switch Connection Control (SCC) policy, sets Insistent Domain ID, and sets the Fabric Wide Consistency Policy (FWCP) for SCC in strict mode.

For mixed Fabric OS and M-EOS fabrics:

- For Fabric OS switches, HIF activates the SCC policy, sets Insistent Domain ID, and sets the FWCP for SCC in tolerant mode.
- For M-EOS switches, HIF activates Enterprise Fabric Mode, Fabric Binding, Switch Binding, Insistent Domain ID, and RSCNs.

Activating HIF mode enables the following features:

- **Fabric Binding (M-EOS only).** Allows or prohibits switches from merging with a selected fabric.

---

### NOTE

NOTE: Fabric Binding cannot be disabled while HIF is active even if the switch is offline.

---

- **Switch Binding (M-EOS only).** This feature, enabled through a device's Element Manager, allows or prohibits switches from connecting to switch E\_Ports and devices from connecting to F\_Ports.

---

### NOTE

NOTE: Switch binding can be disabled while Enterprise Fabric Mode is active if the switch is offline.

---

- **Switch Connection Control (Fabric OS only).** This feature, enabled through a device's Element Manager, prevents unauthorized switches from joining a fabric.
- **Fabric Wide Consistency Policy (Fabric OS only).** This feature makes sure that switches in the fabric enforce the same policies.
- **Domain RSCNs (M-EOS only).** This feature, enabled through a device's Element Manager, indicates that an event occurred to a switch in a fabric. The only cause would be a switch entering or leaving the fabric. Notifications are sent fabric-wide and are not constrained by a zone set. Domain RSCNs are not sent between end-devices.
- **Insistent Domain ID (Fabric OS and M-EOS).** This feature, enabled through a device's Element Manager, sets the domain ID as the active domain identification when the fabric initializes. When Insistent Domain ID is enabled, the switch isolates itself from the fabric if the preferred domain ID is not assigned as the switch's domain ID.

## High integrity fabric requirements

The term high integrity fabric (HIF) refers to a set of strict, consistent, fabric-wide policies. There are several specific configuration requirements for high integrity fabrics:

- Insistent domain ID (IDID) must be enabled in the participating switches.
- Port-based routing must be used on the participating switches.
- A policy must be set that limits connectivity to only the switches within the same fabric. Fabric binding is a security method for restricting switches that may join a fabric. For Fabric OS switches, fabric binding is implemented by defining a switch connection control (SCC) policy that prevents unauthorized switches from joining a fabric.
- Switch binding is a more secure alternative to fabric binding. It is a security method for restricting devices that connect to a particular switch. Switch binding is available only on M-EOS switches and directors. Switch binding has two options: restrict all, and restrict switches only. Switch binding should only be implemented in FICON environments with the switch restriction only. The difference between switch binding and fabric binding is that with fabric binding a defined switch can join the fabric by connecting to any switch in the fabric while with switch binding the new switch can only join by connecting to a specific switch in the fabric.
- Dynamic Load Sharing (DLS) should be disabled. If DLS is not disabled, DLS automatically adjusts routes when a new ISL is added, and when an ISL is taken offline and brought online again. This process may result in dropped frames.

---

### NOTE

Port binding is a security method for restricting devices that connect to particular switch ports. Port binding should never be used in FICON environments. The FICON channel cannot be added to the port binding list.

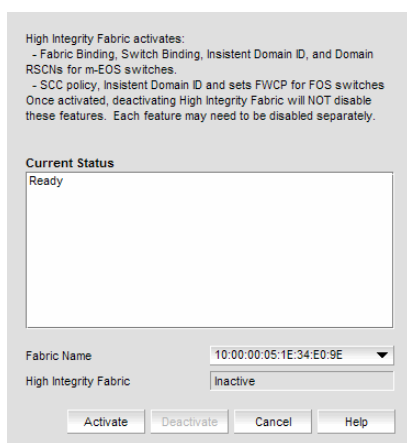
---

## Activating high integrity fabrics

To activate a HIF, complete the following steps.

1. Select **Configure > High Integrity Fabric**.

The **High Integrity Fabric** dialog box displays.



**FIGURE 100** High Integrity Fabric dialog box

2. Select the fabric on which you want to activate HIF from the **Fabric Name** list.

The HIF status displays in the **High Integrity Fabric** field.

3. Click **Activate**.

For Pure Fabric OS fabrics, HIF activates the Switch Connection Control (SCC) policy, sets Insistent Domain ID, and sets the Fabric Wide Consistency Policy (FWCP) for SCC in strict mode.

For mixed Fabric OS and M-EOS fabrics:

- For Fabric OS switches, HIF activates the SCC policy, sets Insistent Domain ID, and sets the FWCP for SCC in tolerant mode.
- For M-EOS switches, HIF activates Enterprise Fabric Mode, Fabric Binding, Switch Binding, Insistent Domain ID, and RSCNs.

## Deactivating high integrity fabrics

---

### NOTE

Deactivating high integrity fabrics is not supported in a pure Fabric OS environment.

---

To deactivate a HIF, complete the following steps.

1. Select **Configure > High Integrity Fabric**.

The **High Integrity Fabric** dialog box displays.

2. Select the fabric on which you want to deactivate HIF from the **Fabric Name** list.

The HIF status displays in the **High Integrity Fabric** field.

3. Click **Deactivate**.

Deactivating HIF on a fabric does not deactivate the features on the individual switches, you must disable them individually:

- For Fabric OS switches, disable the SCC policy, Insistent Domain ID, and the Fabric Wide Consistency Policy for SCC in tolerant mode.
- For M-EOS switches, disable Fabric Binding, Switch Binding, Insistent Domain ID, and RSCNs.

## 9 Deactivating high integrity fabrics

# Fault Management

---

## In this chapter

• Fault management overview.....	247
• Event logs.....	248
• Event policies.....	257
• Event notification.....	274
• SNMP trap and informs registration and forwarding .....	278
• Syslog forwarding.....	283

## Fault management overview

Fault management enables you to monitor your SAN using the following methods:

- Monitor logs for specified conditions and notify you or run a script when the specified condition is met.
- Create event-based policies, which contain an event trigger and action.
- Configure E-mail event notification.
- Listen, forward, and process SNMP traps from Fabric OS switches, which eliminates the need to poll switches for events.
- Receive and forward Syslog messages from Fabric OS switches and Brocade HBAs (managed using HCM Agent).

Fault management also supports application events.

## Event logs

The Management application provides a variety of logs through which you can monitor the SAN.

You can view all events that take place in the SAN through the Master Log at the bottom of the main window. You can also view a specific log by selecting an option from the **Monitor** menu's **Logs** submenu. The logs are described in the following list:

- **Audit Log.** Displays all 'Application Events' raised by the application modules and all Audit Syslog messages from the switches and Brocade HBAs.
- **Event Log.** Displays all 'Product Event' type events from all discovered switches and Brocade HBAs.
- **Fabric Log.** Displays 'Product Events', 'Device Status', and 'Product Audit' type events for all discovered fabrics.
- **FICON Log.** Displays all the 'RLIR' and 'LRIR' type events, for example, 'link incident' type events.
- **Product Status Log.** Displays events which indicate a change in Switch Status for all discovered switches and Brocade HBAs.
- **Security Log.** Displays all security events for the discovered switches.
- **Syslog Log.** Displays syslog messages from switches and HBAs.

The Management application also has an event notification feature. By configuring event notification, you can specify when the application should alert you of an event. For details, refer to [“Configuring e-mail notification”](#) on page 274.

For information about the Master Log interface, fields, and icons, refer to [“Master Log”](#) on page 7.

### Viewing event logs

You can view log data through the Master Log on the main window. However, if you want to see only certain types of events, for example only security events, open a specific log through the **Logs** dialog box.

---

#### NOTE

You can also launch the Fabric logs and the Product Status logs from the Status bar.

---

To view a log, complete the following steps.

1. Select **Monitor > Logs > Log\_Type**.  
The **Log\_Type Logs** dialog box displays the kind of log you selected.
2. Review the information in the log.
3. Click **Close**.

## Copying part of a log entry

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy part of a log, complete the following steps.

1. Select **Monitor > Logs > Log\_Type**.

The *Log\_Type* **Logs** dialog box displays the kind of log you selected.

2. Select the rows you want to copy.
  - To select contiguous rows, select the first row you want to copy, press Shift, and click the contiguous row or rows you want to copy.
  - To select non-contiguous rows, select the first row you want to copy, press CTRL, and click the additional row or rows you want to copy.
3. Right-click one of the selected rows and select **Copy Rows**.
4. Open the application to which you want to paste the data.
5. Click where you want to paste the data.
6. Press CTRL+V (or select **Edit > Paste** from the other application).

All data and column headings are pasted.
7. Click **Close** to close the dialog box.

## Copying an entire log entry

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy a log, complete the following steps.

1. Select **Monitor > Logs > Log\_Type**.

The *Log\_Type* **Logs** dialog box displays the kind of log you selected.

2. Right-click a row and select **Copy Table**.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press CTRL+V (or select **Edit > Paste** from the other application).

All data and column headings are pasted.
6. Click **Close** to close the dialog box.

## Exporting the entire log

You can export the log data to a tab delimited text file.

To export a log, complete the following steps.

1. Select **Monitor > Logs > Log\_Type**.  
The *Log\_Type Log* dialog box displays the kind of log you selected.
2. Right-click a row and select **Export Table**.  
The **Save table to a tab delimited file** dialog box displays.
3. Browse to the location where you want to export the data.
4. Enter a name for the file in the **File Name** field.
5. Click **Save**.  
All data and column headings are exported to the text file.
6. Click **Close** to close the dialog box.

## E-mailing all event details from the Master Log

---

### NOTE

You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to [“Configuring e-mail notification”](#) on page 274.

---

To e-mail event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **E-mail > All**.  
The **E-mail** dialog box displays.
3. Enter the e-mail address of the person to receive the e-mail in the **To** field.
4. Enter your e-mail address in the **From** field.
5. Click **OK**.

## E-mailing selected event details from the Master Log

---

### NOTE

You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to [“Configuring e-mail notification”](#) on page 274.

---

To e-mail event details from the Master Log, complete the following steps.

1. Select the events that you want to e-mail.
2. Right-click the selected events in the Master Log.
3. Select **E-mail > Selection**.  
The **E-mail** dialog box displays.
4. Enter the e-mail address of the person to receive the e-mail in the **To** field.

5. Enter your e-mail address in the **From** field.
6. Click **OK**.

## E-mailing a range of event details from the Master Log

### NOTE

You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to [“Configuring e-mail notification”](#) on page 274.

To e-mail event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **E-mail > Date**.  
The **E-mail** dialog box displays.
3. Select the date range for the event details you want to e-mail in the **Range** from and to fields.
4. Enter the e-mail address of the person to receive the e-mail in the **To** field.
5. Enter your e-mail address in the **From** field.
6. Click **OK**.

## Displaying event details from the Master Log

You can view detailed information for an event.

To display event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Display Details**.  
The **Event Details** dialog box displays.
3. Review the information.

**TABLE 17** Event details

Event Field	Description
<b>Count</b>	Number of times this event occurred on the host.
<b>Resolved</b>	Whether or not the event has been resolved.
<b>Message</b>	The message associated with the event.
<b>Time (Switch)</b>	The time the event occurred and the switch on which it occurred.
<b>Probable Cause</b>	The probable cause of the event.
<b>Module Name</b>	The module name.
<b>Event Source</b>	The event source.
<b>Audit</b>	The audit.
<b>Status</b>	The switch operational status.
<b>Severity</b>	The event severity.
<b>Source Name</b>	The source of the event.

**TABLE 17** Event details (Continued)

Event Field	Description
Virtual Fabric ID	The virtual fabric identifier.
Message ID	The message text.
Recommended Action	The recommended action.
Contributors	The contributor to this event.
Time (Host)	The time this event occurred and the host on which it occurred.

4. Click **Close** to close the **Event Details** dialog box.

## Copying part of the Master Log

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy part of the Master Log, complete the following steps.

1. Select the rows you want to copy in the Master Log.
    - To select contiguous rows, select the first row you want to copy, press Shift, and click the contiguous row or rows you want to copy.
    - To select non-contiguous rows, select the first row you want to copy, press CTRL, and click the additional row or rows you want to copy.
  2. Right-click one of the selected rows and select **Table > Copy Rows**.
  3. Open the application to which you want to paste the data.
  4. Click where you want to paste the data.
  5. Press CTRL+V (or select **Edit > Paste** from the other application).
- All data and column headings are pasted.

## Copying the entire Master Log

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
  2. Select **Table > Copy Table**.
  3. Open the application to which you want to paste the data.
  4. Click where you want to paste the data.
  5. Press CTRL+V (or select **Edit > Paste** from the other application).
- All data and column headings are pasted.

## Exporting the Master Log

You can export the Master Log to a tab delimited text file. Use this to analyze or store the data using another tool.

To export the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Table > Export Table**.

The **Save table to a tab delimited file** dialog box displays.

3. Browse to the location where you want to export the data.
4. Enter a name for the file in the **File Name** field.
5. Click **Save**.

All data and column headings are exported to the text file.

6. Click **Close** to close the dialog box.

## Filtering events in the Master Log

You can filter the events that display in the Master Log on the main window. By default, all event types display in the **Selected Events** table.

For more information about the Master Log, refer to [“Master Log”](#) on page 7.

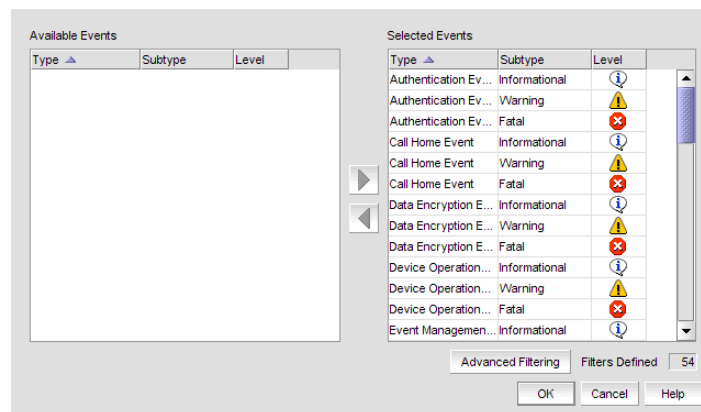
### NOTE

The e-mail filter in the Management application is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box.

To filter events, complete the following steps.

1. Click the **Filter** hyper link in the Master Log.

The **Define Filter** dialog box displays ([Figure 101](#)).



**FIGURE 101** Define Filter dialog box

## 10 Setting up advanced event filtering for the Master Log

2. Select from the following to include or exclude event types.
  - To include an event type in the filter, select the event from the **Available Events** table and click the right arrow.
  - To exclude an event type from the filter, select the event from the **Selected Events** table and click the left arrow.
3. Click **OK**.
4. Select one of the following to determine what view to filter events.
  - Select the **Filter** check box to view only the events specified in the **Define Filter** dialog box, regardless of the current view.
  - Select the **Only events for current view** check box to view only the events specified in the **Define Filter** dialog box for products in the current view.

### NOTE

Selecting these options only filters application and product-specific events.

Clear both the **Filter** and **Only events in current view** check boxes to turn off the filter and view all events.

## Setting up advanced event filtering for the Master Log

To set up advanced event filtering on the selected events for the Master Log, complete the following steps.

1. Click the **Filter** hyper link in the Master Log.

The **Define Filter** dialog box displays.
2. Click **Advanced Filtering**.

The **Advanced Event Filtering** dialog box displays.
3. Click the **Include Events** tab and complete the following steps.

Include Events | Exclude Events

To only display events that meet certain criterion, select the event type, select the event column, enter value for the selected column, and move to the Additional Filters list.

**Define Filter**

Event Type: Config Management Event  
Event Column: Fabric Name  
Value Contains: DF

**Additional Filters - include these Events**

Event Type	Event Column	Value Co
Config Management Event	Fabric Name	DF
Call Home Event	Fabric Name	DF

Remove

☒ Last: All Hours  
☐ Between: 3/2/10 2:34 PM and 3/3/10 2:34 PM

OK Cancel Help

**FIGURE 102** Advanced Event Filtering dialog box - Include Events tab

- a. Select the event type you want to include from the **Event Type** list.

All event types are listed in alphabetical order.

- b. Select the event column for the event from the **Event Column** list.  
All event columns are listed in alphabetical order.
- c. Enter all or part of the event type value in the **Value Contains** text box.
- d. Click the right arrow button to move the event type to the **Additional Filters - Include these Events** table.  
To add additional filters, repeat steps a through d.

**NOTE**

You can configure a maximum of 10 filters to be included.

To remove a filter from the **Additional Filters - Include these Events** table, refer to [“Removing an advanced event filter”](#) on page 256.

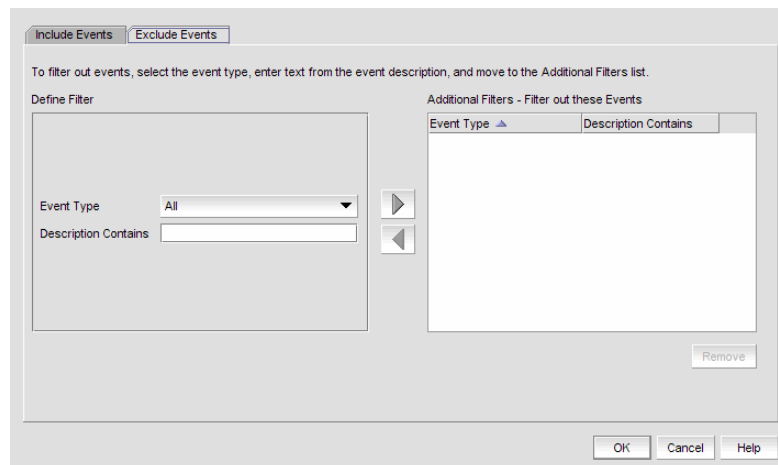
4. Configure a date and time-based filter by choosing one of the following options:

**NOTE**

The date and time-based filter fields do not display unless there is at least one advanced filter in the **Additional Filters - Include these Events** table.

- To set a duration for the filters, select **Last** and choose how long to filter the events from the list. Options include **All**, **1 hour**, **2 hours**, **12 hours**, and **24 hours**.
- To set a specific date and time for the filters, select **Between** and enter a start and end time in the appropriate fields.

5. Click the **Exclude Events** tab and complete the following steps.



**FIGURE 103** Advanced Event Filtering dialog box - Include Events tab

- a. Select the event type you want to remove from the **Event Type** list.  
All event types are listed in alphabetical order.
- b. Enter all or part of the event type description text in the **Description Contains** text box (up to 40 characters).  
This text should be the same text that displayed in the **Description** field for the events that displayed on the Master Log.

## 10 Removing an advanced event filter

- c. Click the right arrow button to move the event type to the **Additional Filters - Filter out these Events** table.

---

**NOTE**

You can configure a maximum of 10 filters to be excluded.

---

6. Click **OK**.  
The **Define Filter** dialog box displays.
7. Click **OK** to close **Define Filter** dialog box.

### Removing an advanced event filter

To remove an advanced event filter, complete the following steps.

1. Click the **Filter** hyper link in the Master Log.  
The **Define Filter** dialog box displays.
2. Click **Advanced Filtering**.  
The **Advanced Event Filtering** dialog box displays.
3. Click the **Include Events** tab, if necessary.
4. Select the filter you want to remove from the **Additional Filters - Include these Events** table.

---

**NOTE**

You can configure a maximum of 10 filters each on the **Include Events** tab and **Exclude Events** tab.

---

5. Click **Remove**.
6. Click **Yes** on the 'remove the filters' message.
7. Click **OK** to close the **Advanced Event Filtering** dialog box.  
The **Define Filter** dialog box displays.
8. Click **OK** to close **Define Filter** dialog box.

## Event policies

You can create policies for events you want to monitor. A policy is the mechanism defined by you that identifies the response to specific event types. You can customize the event management policy using triggers and actions, which are explained in this section. You can create a maximum of 10 policies at a time.

### Policy types

You can configure event policies for the following policy types:

- Event — use to configure triggers and actions for the following “[Event types](#)”.
- Port Offline — use to configure triggers and actions for Port.
- PM Threshold Crossed — use to configure triggers and actions for performance thresholds.
- Security Violation — use to configure triggers and actions for security violations.

### *Event types*

You can configure triggers and actions for the following event types:

- Authentication Event — occurs when an authentication event has been triggered.
- Call Home Event — occurs when a call home event has been triggered.
- Config Management Event — occurs when a configuration management event has been triggered
- Data Encryption Event — occurs when a data encryption event has been triggered.
- Device Status Event — notifies you of the operational status of SAN products.
- Fabric Event — notifies you of fabric changes.
- Fault Management Event — occurs when an event policy has been triggered.
- FICON Event — occurs when a FICON event has been triggered
- Link Incident Event — notifies you of changes to the link status.
- Management Server Event — occurs when a management server event has been triggered
- Performance Event — occurs when the performance at a switch port crosses a defined threshold.
- Port Fencing Event — occurs when a port fencing event has been triggered
- Product Audit Event — occurs when a target product is audited.
- Product Event — notifies you when the product status changes.
- Product Open Trunking Event — occurs when a device open trunking event has been triggered.
- Product State Event — occurs when a device or connection changes to Up or Down.
- Product Threshold Alert Event — notifies you when a threshold alert has been reached.
- Security Event — notifies you when a product’s security level changes.
- Software Exception Event — occurs when a software exception event has been triggered.
- Tech Support Event — occurs when a technical support event is triggered.
- User Action Event — occurs when you change a setting in the Server.
- Zoning Event — occurs when a zoning event has been triggered.

## Policy triggers

A trigger is a logical filter that determines which conditions will initiate a set of predefined actions. You can set multiple triggers. The Management application enables you to set the following triggers:

- **IP Address** — Initiates the defined action when the IP address of a device is encountered.
- **Node WWN** — Initiates the defined action when the Node WWN of a device is encountered.
- **Name** — Initiates the defined action when the Name (user-defined) of a device is encountered.

## Policy actions

You can automate tasks that you perform on the SAN by configuring multiple actions to be performed when an associated trigger is fired. The following actions are available:

- **Broadcast Message** — Displays a message to all open Clients.
- **Launch Script** — Launches the specified application using a script.

---

### NOTE

Launch scripts with a user interface or a Network file launch are not supported.

---

- **Send E-mail** — Sends an e-mail message to specified recipients.
- **Capture Support Data (Fabric OS)** — Triggers supportSave capture.

## Adding an event policy

To add an event policy, complete the following steps.

1. Select **Monitor > Event Policies**.

The **Event Policies** dialog box displays.

2. Click **Add**.

The **Add Event Policy** dialog box displays.

3. Enter a name (1024 characters maximum) for the policy in the **Name** field.

Policy names must be unique; however, they are case insensitive.

4. Enter a description (1024 characters maximum) for the policy in the **Description** field.

5. Select **Event** from the **Policy Type** list.

6. Select an event type from the **Event Type** list.

For a list of event types, refer to [“Event types”](#) on page 257.

7. Select an event level (ERROR, WARNING, or INFO) from the **Event Level** list.

8. Enter all or part of the event description text (1024 characters maximum) in the **Description Contains** field.

This entry can be from the start, middle, or end of the event description. If the entry matches or is part of the event description, the policy is triggered.

9. Enter all or part of the message ID associated with SNMP traps and Syslog messages in the **Message ID** field.  
If the entry matches or is part of the message ID, the policy is triggered.
10. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.  
The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches in the event and all other conditions are met, an action is triggered.  
IP addresses can either be in IPv4 or IPv6 format and must be complete.  
A Node WWN is accepted with or without the colon.
11. Enter a value (between 2 and 999) in the **Count** field.
12. Enter a value (between 1 and 999) in the **Duration** field.
13. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.  
The maximum duration is 30 minutes.
14. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.  
For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.
15. Click **OK** on the **Add Event Policy** dialog box.
16. Select the **Active** check box for the policy you want to activate.
17. Click **OK** on the **Event Policies** dialog box.

## Adding an Port offline policy

To add an Port offline policy, complete the following steps.

1. Select **Monitor > Event Policies**.  
The **Event Policies** dialog box displays.
2. Click **Add**.  
The **Add Event Policy** dialog box displays.
3. Enter a name (1024 characters maximum) for the policy in the **Name** field.  
Policy names must be unique; however, they are case insensitive.
4. Enter a description (1024 characters maximum) for the policy in the **Description** field.
5. Select **Port Offline** from the **Policy Type** list.

6. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.  
 The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.  
 IP addresses can either be in IPv4 or IPv6 format and must be complete.  
 A Node WWN is accepted with or without the colon.
7. Enter a value (between 2 and 999) in the **Count** field.
8. Enter a value (between 1 and 999) in the **Duration** field.
9. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.  
 The maximum duration is 30 minutes.
10. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.  
 For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.
11. Click **OK** on the **Add Event Policy** dialog box.
12. Select the **Active** check box for the policy you want to activate.
13. Click **OK** on the **Event Policies** dialog box.

## Adding a PM threshold crossed policy

To add a PM threshold crossed policy, complete the following steps.

1. Select **Monitor > Event Policies**.  
 The **Event Policies** dialog box displays.
2. Click **Add**.  
 The **Add Event Policy** dialog box displays.
3. Enter a name (1024 characters maximum) for the policy in the **Name** field.  
 Policy names must be unique; however, they are case insensitive.
4. Enter a description (1024 characters maximum) for the policy in the **Description** field.
5. Select **PM Threshold Crossed** from the **Policy Type** list.
6. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.  
 The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.  
 IP addresses can either be in IPv4 or IPv6 format and must be complete.  
 A Node WWN is accepted with or without the colon.
7. Enter a value (between 2 and 999) in the **Count** field.
8. Enter a value (between 1 and 999) in the **Duration** field.

9. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

The maximum duration is 30 minutes.

10. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.

11. Click **OK** on the **Add Event Policy** dialog box.
12. Select the **Active** check box for the policy you want to activate.
13. Click **OK** on the **Event Policies** dialog box.

## Adding a security violation policy

To add a security violation policy, complete the following steps.

1. Select **Monitor > Event Policies**.

The **Event Policies** dialog box displays.

2. Click **Add**.

The **Add Event Policy** dialog box displays.

3. Enter a name (255 characters maximum) for the policy in the **Name** field.

Policy names must be unique; however, they are case insensitive.

4. Enter a description (255 characters maximum) for the policy in the **Description** field.

5. Select **Security Violation** from the **Policy Type** list.

6. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

IP addresses can either be in IPv4 or IPv6 format and must be complete.

A Node WWN is accepted with or without the colon.

7. Enter a value (between 2 and 999) in the **Count** field.
8. Enter a value (between 1 and 999) in the **Duration** field.
9. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

The maximum duration is 30 minutes.

10. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.

11. Click **OK** on the **Add Event Policy** dialog box.
12. Select the **Active** check box for the policy you want to activate.
13. Click **OK** on the **Event Policies** dialog box.

### Defining the broadcast message action

You can define the content of the broadcast message that occurs when a policy is triggered. You can only edit actions from the **Add Event Policy**, **Duplicate Event Policy**, or **Edit Event Policy** dialog boxes.

For step-by-step instructions on adding or editing an event policy, refer to [“Adding an event policy”](#) on page 258, [“Adding an Port offline policy”](#) on page 259, [“Adding a PM threshold crossed policy”](#) on page 260, or [“Adding a security violation policy”](#) on page 261.

For step-by-step instructions on duplicating an event policy, refer to [“Duplicating an event policy”](#) on page 266, [“Duplicating an Port offline policy”](#) on page 267, [“Duplicating a PM threshold crossed policy”](#) on page 268, or [“Duplicating a security violation policy”](#) on page 269.

For step-by-step instructions on editing an event policy, refer to [“Editing an event policy”](#) on page 270, [“Editing an Port offline policy”](#) on page 271, [“Editing a PM threshold crossed policy”](#) on page 272, or [“Editing a security violation policy”](#) on page 273.

To define the broadcast message, complete the following steps.

1. Select **Broadcast Message** from the **Actions** list.
2. Click **Configure**.

The **Broadcast Message** dialog box displays.

3. Select a severity (error, warning, or informational) for the message from the **Severity** list.
4. Enter a message to be displayed when the policy is triggered in the **Message Content** field.

You can enter 256 characters for the broadcast message. The following special characters are not allowed: ~ ' ! @ \$ ^ & + = { } [ ] | \ ' < > / “

5. Click **OK** on the **Broadcast Message** dialog box.
6. Click **OK** on the **Add**, **Duplicate**, or **Edit Event Policy** dialog box.

## Defining the launch script action

---

### NOTE

Launch scripts with a user interface are not supported.

---

You can define the path to the script that is launched when a policy is triggered. When the script launches, the Management application does not verify the existence of the script.

The script must have the following characteristics:

- It must reside on the Management application server.
- It must be capable of being executed by the OS where the Management application server is installed and it must be a valid binary for that OS (Windows, Solaris, or Linux).

You can only edit actions from the **Add Event Policy**, **Duplicate Event Policy**, or **Edit Event Policy** dialog boxes.

For step-by-step instructions on adding or editing an event policy, refer to [“Adding an event policy”](#) on page 258, [“Adding an Port offline policy”](#) on page 259, [“Adding a PM threshold crossed policy”](#) on page 260, or [“Adding a security violation policy”](#) on page 261.

For step-by-step instructions on duplicating an event policy, refer to [“Duplicating an event policy”](#) on page 266, [“Duplicating an Port offline policy”](#) on page 267, [“Duplicating a PM threshold crossed policy”](#) on page 268, or [“Duplicating a security violation policy”](#) on page 269.

For step-by-step instructions on editing an event policy, refer to [“Editing an event policy”](#) on page 270, [“Editing an Port offline policy”](#) on page 271, [“Editing a PM threshold crossed policy”](#) on page 272, or [“Editing a security violation policy”](#) on page 273.

To define the launch script path, complete the following steps.

1. Select **Launch Script** from the **Actions** list.
2. Click **Configure**.

The **Launch Script** dialog box displays.

3. Enter the full path (including executable) of the launch script in the **File Name** field.

---

### NOTE

Launch scripts with a user interface or a Network file launch are not supported.

---

You must enter a fully qualified path on the Management application Server for Windows (for example, C:\Program Files\Management\_Application\_Name 10.X.X\bin\xyz.bat) as well as Linux and Solaris (for example, /etc/proc/sbin/script.sh).

4. Select the check box to send event parameters (Level, Source Name, Source Address, Type, and Description) as arguments.
5. Click **OK** on the **Launch Script** dialog box.

---

### NOTE

The Management application does not verify that the file name exists in the specified folder.

---

6. Click **OK** on the **Add**, **Duplicate**, or **Edit Event Policy** dialog box.

## Defining the send e-mail action

You can define the content of the e-mail message that occurs when a policy is triggered. You can only edit actions from the **Add Event Policy**, **Duplicate Event Policy**, or **Edit Event Policy** dialog boxes.

For step-by-step instructions on adding or editing an event policy, refer to [“Adding an event policy”](#) on page 258, [“Adding an Port offline policy”](#) on page 259, [“Adding a PM threshold crossed policy”](#) on page 260, or [“Adding a security violation policy”](#) on page 261.

For step-by-step instructions on duplicating an event policy, refer to [“Duplicating an event policy”](#) on page 266, [“Duplicating an Port offline policy”](#) on page 267, [“Duplicating a PM threshold crossed policy”](#) on page 268, or [“Duplicating a security violation policy”](#) on page 269.

For step-by-step instructions on editing an event policy, refer to [“Editing an event policy”](#) on page 270, [“Editing an Port offline policy”](#) on page 271, [“Editing a PM threshold crossed policy”](#) on page 272, or [“Editing a security violation policy”](#) on page 273.

You must configure the Management application e-mail server before you can define the e-mail action. For more information, refer to [“Configuring e-mail notification”](#) on page 274.

To define the e-mail message, complete the following steps.

1. Select **Send E-mail** from the **Actions** list.
2. Click **Configure**.

The **Send E-Mail** dialog box displays.

3. Enter the e-mail address of the person you want to receive this message when the trigger occurs in the **To** field.
4. Enter your e-mail address in the **From** field.
5. Enter a subject for the e-mail message in the **Subject** field.
6. Enter a message to be displayed when the policy is triggered in the **Message** field.

You can enter 256 characters for the e-mail message. The following special characters are not allowed: ~ ' ! @ \$ ^ & + = { } [ ] | \ ' < > / : “

7. Click **OK** on the **Send E-Mail** dialog box.
8. Click **OK** on the **Add**, **Duplicate**, or **Edit Event Policy** dialog box.

## Configuring support data capture action

You can configure the Management application to start supportSave capture on Fabric OS devices when a policy is triggered. You can only edit actions from the **Add Event Policy**, **Duplicate Event Policy**, or **Edit Event Policy** dialog boxes.

For step-by-step instructions on adding or editing an event policy, refer to [“Adding an event policy”](#) on page 258, [“Adding an Port offline policy”](#) on page 259, [“Adding a PM threshold crossed policy”](#) on page 260, or [“Adding a security violation policy”](#) on page 261.

For step-by-step instructions on duplicating an event policy, refer to [“Duplicating an event policy”](#) on page 266, [“Duplicating an Port offline policy”](#) on page 267, [“Duplicating a PM threshold crossed policy”](#) on page 268, or [“Duplicating a security violation policy”](#) on page 269.

For step-by-step instructions on editing an event policy, refer to [“Editing an event policy”](#) on page 270, [“Editing an Port offline policy”](#) on page 271, [“Editing a PM threshold crossed policy”](#) on page 272, or [“Editing a security violation policy”](#) on page 273.

To configure the Management application to start supportSave on Fabric OS devices, complete the following steps.

---

### NOTE

If you select **User Action Event** or **Tech Support Event** from the **Event Type** list, **Capture Support Data (Fabric OS)** cannot be configured to start supportSave capture.

---

1. Select **Capture Support Data (Fabric OS)** from the **Actions** list.
2. Click **OK** on the message.  
Note that capture support data is only triggered for Fabric OS switch events.
3. Click **OK** on the **Add**, **Duplicate**, or **Edit Event Policy** dialog box.

## Activating a policy

1. Select **Monitor > Event Policies**.  
The **Event Policies** dialog box displays.
2. Select the **Active** check box for each policy you want to activate.  
If the policy actions have not been selected an error message displays. For step-by-step instructions, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, or [“Defining the send e-mail action”](#) on page 264.
3. Click **OK** on the **Event Policies** dialog box.

## Deactivating a policy

1. Select **Monitor > Event Policies**.  
The **Event Policies** dialog box displays.
2. Clear the **Active** check box for each policy you want to deactivate.
3. Click **OK** on the **Event Policies** dialog box.

### Deleting a policy

1. Select **Monitor > Event Policies**.  
The **Event Policies** dialog box displays.
2. Select the policy you want to delete.  
Press Ctrl and then click to select more than one policy.
3. Click **Delete**.
4. Click **OK** on the **Event Policies** dialog box.

### Duplicating an event policy

To duplicate an event policy, complete the following steps.

1. Select **Monitor > Event Policies**.  
The **Event Policies** dialog box displays.
2. Select the policy you want to duplicate in the **Policies** table.
3. Click **Duplicate**.  
The **Duplicate Event Policy** dialog box displays.
4. Enter a name (255 characters maximum) for the policy in the **Name** field.  
Policy names must be unique; however, they are case insensitive.
5. Edit the description (255 characters maximum) for the policy in the **Description** field.
6. Change the event type by selecting an event type from the **Event Type** list.  
For a list of event types, refer to [“Event types”](#) on page 257.
7. Change the event level by selecting an event level from the **Event Level** list.
8. Edit the event description text (255 characters maximum) in the **Description Contains** field.  
This entry can be from the start, middle, or end of the event description. If the entry matches or is part of the event description, the policy is triggered.
9. Edit the message ID associated with SNMP traps and Syslog messages in the **Message ID** field.  
If the entry matches or is part of the message ID, the policy is triggered.

10. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

IP addresses can either be in IPv4 or IPv6 format and must be complete.

A Node WWN is accepted with or without the colon.

11. Change the count value (between 2 and 999) in the **Count** field.
12. Change the duration value (between 1 and 999) in the **Duration** field.
13. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

The maximum duration is 30 minutes.

14. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.

15. Click **OK** on the **Edit Event Policy** dialog box.
16. Select the **Active** check box to activate the duplicated policy.
17. Click **OK** on the **Event Policies** dialog box.

## Duplicating an Port offline policy

To duplicate an Port offline policy, complete the following steps.

1. Select **Monitor > Event Policies**.

The **Event Policies** dialog box displays.

2. Select the policy you want to duplicate in the **Policies** table.
3. Click **Duplicate**.

The **Duplicate Event Policy** dialog box displays.

4. Enter a name (255 characters maximum) for the policy in the **Name** field.

Policy names must be unique; however, they are case insensitive.

5. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

IP addresses can either be in IPv4 or IPv6 format and must be complete.

A Node WWN is accepted with or without the colon.

6. Change the count value (between 2 and 999) in the **Count** field.
7. Change the duration value (between 1 and 999) in the **Duration** field.

8. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.  
The maximum duration is 30 minutes.
9. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.  
  
For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.
10. Click **OK** on the **Edit Event Policy** dialog box.
11. Select the **Active** check box to activate the duplicated policy.
12. Click **OK** on the **Event Policies** dialog box.

## Duplicating a PM threshold crossed policy

To duplicate a PM threshold crossed policy, complete the following steps.

1. Select **Monitor > Event Policies**.  
The **Event Policies** dialog box displays.
2. Select the policy you want to duplicate in the **Policies** table.
3. Click **Duplicate**.  
The **Duplicate Event Policy** dialog box displays.
4. Enter a name (255 characters maximum) for the policy in the **Name** field.  
Policy names must be unique; however, they are case insensitive.
5. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.  
  
The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.  
  
IP addresses can either be in IPv4 or IPv6 format and must be complete.  
  
A Node WWN is accepted with or without the colon.
6. Change the count value (between 2 and 999) in the **Count** field.
7. Change the duration value (between 1 and 999) in the **Duration** field.
8. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.  
The maximum duration is 30 minutes.
9. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.  
  
For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.
10. Click **OK** on the **Add Event Policy** dialog box.

11. Select the **Active** check box to activate the duplicated policy.
12. Click **OK** on the **Event Policies** dialog box.

## Duplicating a security violation policy

To duplicate a security violation policy, complete the following steps.

1. Select **Monitor > Event Policies**.

The **Event Policies** dialog box displays.

2. Select the policy you want to duplicate in the **Policies** table.
3. Click **Duplicate**.

The **Duplicate Event Policy** dialog box displays.

4. Enter a name (255 characters maximum) for the policy in the **Name** field.

Policy names must be unique; however, they are case insensitive.

5. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

IP addresses can either be in IPv4 or IPv6 format and must be complete.

A Node WWN is accepted with or without the colon.

6. Enter a value (between 2 and 999) in the **Count** field.
7. Enter a value (between 1 and 999) in the **Duration** field.
8. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

The maximum duration is 30 minutes.

9. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.

10. Click **OK** on the **Add Event Policy** dialog box.
11. Select the **Active** check box to activate the duplicated policy.
12. Click **OK** on the **Event Policies** dialog box.

## Editing an event policy

To edit an event policy, complete the following steps.

1. Select **Monitor > Event Policies**.

The **Event Policies** dialog box displays.

2. Select the policy you want to edit in the **Policies** table.

3. Click **Edit**.

The **Edit Event Policy** dialog box displays.

---

### NOTE

You cannot edit the event policy name.

---

4. Edit the description (255 characters maximum) for the policy in the **Description** field.

5. Change the event type by selecting an event type from the **Event Type** list.

For a list of event types, refer to [“Event types”](#) on page 257.

6. Change the event level by selecting an event level from the **Event Level** list.

7. Edit the event description text (255 characters maximum) in the **Description Contains** field.

This entry can be from the start, middle, or end of the event description. If the entry matches or is part of the event description, the policy is triggered.

8. Edit the message ID associated with SNMP traps and Syslog messages in the **Message ID** field.

If the entry matches or is part of the message ID, the policy is triggered.

9. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

IP addresses can either be in IPv4 or IPv6 format and must be complete.

A Node WWN is accepted with or without the colon.

10. Change the count value (between 2 and 999) in the **Count** field.

11. Change the duration value (between 1 and 999) in the **Duration** field.

12. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

The maximum duration is 30 minutes.

13. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.

14. Click **OK** on the **Edit Event Policy** dialog box.

15. Select the **Active** check box to activate the modified policy.

16. Click **OK** on the **Event Policies** dialog box.

## Editing an Port offline policy

To edit an Port offline policy, complete the following steps.

1. Select **Monitor > Event Policies**.

The **Event Policies** dialog box displays.

2. Select the policy you want to edit in the **Policies** table.

3. Click **Edit**.

The **Edit Event Policy** dialog box displays.

4. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

IP addresses can either be in IPv4 or IPv6 format and must be complete.

A Node WWN is accepted with or without the colon.

5. Change the count value (between 2 and 999) in the **Count** field.
6. Change the duration value (between 1 and 999) in the **Duration** field.
7. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

The maximum duration is 30 minutes.

8. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.

9. Click **OK** on the **Edit Event Policy** dialog box.
10. Select the **Active** check box to activate the policy.
11. Click **OK** on the **Event Policies** dialog box.

## Editing a PM threshold crossed policy

To edit a PM threshold crossed policy, complete the following steps.

1. Select **Monitor > Event Policies**.

The **Event Policies** dialog box displays.

2. Select the policy you want to edit in the **Policies** table.

3. Click **Edit**.

The **Edit Event Policy** dialog box displays.

4. Edit the trigger in the **IP Address**, **Node WWN**, and **Name** list.

The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

IP addresses can either be in IPv4 or IPv6 format and must be complete.

A Node WWN is accepted with or without the colon.

5. Change the count value (between 2 and 999) in the **Count** field.
6. Change the duration value (between 1 and 999) in the **Duration** field.
7. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

The maximum duration is 30 minutes.

8. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.

9. Click **OK** on the **Add Event Policy** dialog box.
10. Select the **Active** check box to activate the policy.
11. Click **OK** on the **Event Policies** dialog box.

## Editing a security violation policy

To edit a security violation policy, complete the following steps.

1. Select **Monitor > Event Policies**.

The **Event Policies** dialog box displays.

2. Select the policy you want to edit in the **Policies** table.

3. Click **Edit**.

The **Edit Event Policy** dialog box displays.

4. Define the trigger in the **IP Address**, **Node WWN**, and **Name** list.

The trigger is limited to 1024 characters. Multiple values must be separated by a semi-colon. When multiple values are entered, as long as at least one value matches the IP address, Node WWN, or Name in the event and all other conditions are met, an action is triggered.

IP addresses can either be in IPv4 or IPv6 format and must be complete.

A Node WWN is accepted with or without the colons.

5. Enter a value (between 2 and 999) in the **Count** field.
6. Enter a value (between 1 and 999) in the **Duration** field.
7. Select the duration type (**Seconds** or **Minutes**) from the **Duration** list.

The maximum duration is 30 minutes.

8. Select the check box in the **Actions** list for each action you want to occur when this policy is triggered.

For a list of the available actions, refer to [“Policy actions”](#) on page 258. To define an action, refer to [“Defining the broadcast message action”](#) on page 262, [“Defining the launch script action”](#) on page 263, [“Defining the send e-mail action”](#) on page 264, or [“Configuring support data capture action”](#) on page 265.

9. Click **OK** on the **Add Event Policy** dialog box.
10. Select the **Active** check box to activate the policy.
11. Click **OK** on the **Event Policies** dialog box.

## Viewing events

The **All Events** dialog box enables you to view all events that have occurred on the selected switch, even events that were filtered using advanced filtering criteria.

---

### NOTE

You can only create up to 10 events.

---

To view events for a selected device, complete the following steps.

1. Right-click a switch from the device tree or connectivity map.
2. Select **Events** from the list.

The **All Events** dialog box displays.

# Event notification

The Management application records the SAN events in the Master Log. You can configure the application to send event notifications to e-mail addresses at certain time intervals. This is a convenient way to keep track of events that occur on the SAN. You can also configure products to “call home” for certain events, notifying the service center of product problems. For instructions about configuring call home for events, refer to “[Call Home](#)” on page 105.

## Configuring e-mail notification

To send notification of events to users, complete the following steps.

1. Select **Monitor > Event Notification > E-mail**.

The **E-mail Event Notification Setup** dialog box displays ([Figure 104](#)).

☐ Enable E-mail Event Notification

E-mail Server

SMTP over SSL ☐

SMTP Port

\*SMTP ID

\*SMTP Password

Reply Address

Summary Interval  seconds

E-mail Test Options ☒ Send to

☐ Send to all users enabled for notification

\*Fields are optional unless SMTP server enables authentication.

**FIGURE 104** E-mail Notification Setup dialog box

2. Select the **Enable E-mail Event Notification** check box.
3. Enter the IP address or the name of the SMTP mail server that the Server can use to send the e-mail in the **E-mail Server** field.
4. Select the **SMTP over SSL** check box to enable secure communication.
5. Enter the authentication ID of the SMTP mail server in the **SMTP ID** field.

**NOTE**

This field is optional unless the SMTP server enables authentication.

6. Enter the authentication password of the SMTP mail server in the **SMTP Password** field.

**NOTE**

This field is optional unless the SMTP server enables authentication.

7. Enter the recipient’s e-mail address in the **Reply Address** field.

8. Enter the length of time the application should wait between notifications in the **Summary Interval** field and list.

Notifications are combined into a single e-mail and sent at each interval setting. An interval setting of zero causes notifications to be sent immediately.

---

**ATTENTION**

Setting too short an interval can cause the recipient's e-mail inbox to fill very quickly.

---

9. Select one of the following options:
  - Select **Send to** and enter an e-mail address for a user to send a test e-mail to a specific user.
  - Select **Send to all users enabled for notification** to send a test e-mail to all users already set to receive notification.

10. Click **Send Test E-mail** to test the e-mail server.

A message displays whether the server was found. If the server was not found, verify that the server address was entered correctly and that the server is running. If you are using an SMTP mail server, also verify that the SMTP ID and password information was entered correctly.

11. Click **OK** to save your work and close the **E-mail Event Notification Setup** dialog box.

## Setting up advanced event filtering for a user

To set up advanced event filtering on the selected events for a user, complete the following steps.

1. Select **Server > Users**.

The **Server Users** dialog box displays.
2. Select a user in the **Users** table and click **Edit**.

The **Edit User** dialog box displays.
3. Select the **E-mail Notification Enable** check box and click the **Filter** link.

The **Define Filter** dialog box displays.
4. Click **Advanced Filtering**.

The **Advanced Event Filtering** dialog box displays.

## 10 Setting up advanced event filtering for a user

### 5. Click the **Include Events** tab.

To only display events that meet certain criterion, select the event type, select the event column, enter value for the selected column, and move to the Additional Filters list.

Define Filter

Event Type: Config Management Event

Event Column: Fabric Name

Value Contains: DF

Additional Filters - include these Events

Event Type	Event Column	Value Co
Config Management Event	Fabric Name	DF
Call Home Event	Fabric Name	DF

Remove

☒ Last: All Hours

☐ Between: 3/2/10 2:34 PM and 3/3/10 2:34 PM

OK Cancel Help

**FIGURE 105** Advanced Event Filtering dialog box - Include Events tab

- Select the event type you want to include from the **Event Type** list.  
All event types are listed in alphabetical order.
  - Select the event column for the event from the **Event Column** list.  
All event columns are listed in alphabetical order.
  - Enter all or part of the event type value in the **Value Contains** text box.
  - Click the right arrow button to move the event type to the **Additional Filters - Filter out these Events** table.  
To add additional filters, repeat steps a through d.
6. To remove a filter from the **Additional Filters - Include these Events** table, refer to Configure a date and time-based filter by choosing one of the following options:

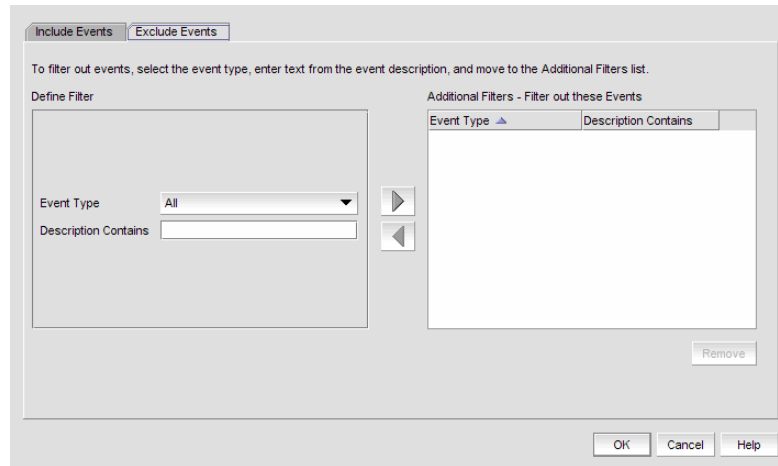
#### NOTE

The date and time-based filter fields do not display unless there is at least one advanced filter in the **Additional Filters - Include these Events** table.

- To set a duration for the filters, select **Last** and choose how long to filter the events from the list. Options include **All**, **1** hour, **2** hours, **12** hours, and **24** hours.
- To set a specific date and time for the filters, select **Between** and enter a start and end time in the appropriate fields.

[“Removing an advanced event filter”](#) on page 256.

7. Click the **Exclude Events** tab.



**FIGURE 106** Advanced Event Filtering dialog box - Include Events tab

- a. Select the event type you want to remove from the **Event Type** list.  
All event types are listed in alphabetical order.
  - b. Enter all or part of the event type description text in the **Description Contains** text box (up to 40 characters).  
This text should be the same text that displayed in the **Description** field for the events that displayed on the Master Log.
  - c. Click the right arrow button to move the event type to the **Additional Filters - Filter out these Events** table.
8. Click **OK**.  
The **Define Filter** dialog box displays.
9. Click **OK** to close **Define Filter** dialog box.

## SNMP trap and informs registration and forwarding

You can configure the application to send SNMP traps and informs to other computers. To correctly configure trap forwarding, you must configure the target computer's IP address and SNMP ports. To correctly configure informs, you must enable informs on the switch.

### Registering the management server

---

**NOTE**

If the source IP address does not match the switch, the Management application does not forward the SNMP traps.

---

---

**NOTE**

SNMP Informs is only supported on Fabric OS 6.3 or later switches discovered through SNMP v3. For information about discovery through SNMP v3, refer to [“Discovering fabrics”](#) on page 36.

---

You can automatically register this server as the trap or informs recipient on all managed Fabric OS devices.

To register the management server, complete the following steps.

1. Select **Monitor > SNMP Setup**.  
The **SNMP Setup** dialog box displays.
2. Click the **Management Server** tab.
3. Select the **Auto register server as SNMP trap or informs recipient** check box, if necessary.  
This check box is selected by default.
4. Enter the SNMP listening port number of the Server in the **SNMP Listening Port (Server)** field, if necessary.  
The default SNMP listening port number is 162 and is automatically populated.
5. Click **OK** on the **SNMP Setup** dialog box.

### Registering a different Management application server

You can register any Management application server as the trap recipient on managed Fabric OS devices. You can register different recipients for different fabrics.

To register a host server, complete the following steps.

1. Select **Monitor > SNMP Setup**.  
The **SNMP Setup** dialog box displays.
2. Click the **Other Recipients** tab.
3. Select **Add** from the **Action** list.
4. Enter the IP address (IPv4 or IPv6 format) of the host server in the **Recipient Server IP Address** field.

5. Select a fabric from the **Targeted Fabric** list.
6. Select a severity (None, Critical, Error, Warning, Info, or Debug) from the **Severity** list.
7. Click **OK** on the **SNMP Setup** dialog box.

## Removing a host server

You can remove any host server as the trap recipient on managed Fabric OS devices.

To remove a host server, complete the following steps.

1. Select **Monitor > SNMP Setup**.  
The **SNMP Setup** dialog box displays.
2. Click the **Other Recipients** tab.
3. Select **Remove** from the **Action** list.
4. Click **OK** on the **SNMP Setup** dialog box.

## Enabling trap forwarding

You can enable trap forwarding on all defined destinations.

To enable trap forwarding, complete the following steps.

1. Select **Monitor > SNMP Setup**.  
The **SNMP Setup** dialog box displays.
2. Click the **Trap Forwarding** tab.
3. Select the **Enable trap forwarding** check box.
4. Click **OK** on the **SNMP Setup** dialog box.

## Adding an SNMPv1 destination

You can only configure six destinations, including v1 and v3 destinations.

To add a V1 destination, complete the following steps.

1. Select **Monitor > SNMP Setup**.  
The **SNMP Setup** dialog box displays.
2. Click the **Trap Forwarding** tab.
3. Select **V1** from the **Trap forwarding type** list.

4. Click **Add**.

The **Add/Edit Trap Recipient** dialog box displays.

- a. (Optional) In the **Description** field, enter a description of the trap recipient.
- b. In the **IP Address** field, enter the trap recipient's IP address.

The Management application accepts IP addresses in IPv4 or IPv6 formats.

- c. Enter the trap recipient's UDP port number, in the **port** field.
- d. Click **OK** on the **Add/Edit Trap Recipient** dialog box.

5. Click **OK** on the **SNMP Setup** dialog box.

### Adding an SNMPv3 destination

You can only configure six destinations, including v1 and v3 destinations.

To add a V3 destination, complete the following steps.

1. Select **Monitor > SNMP Setup**.

The **SNMP Setup** dialog box displays.

2. Click the **Trap Forwarding** tab.
3. Select **V3** from the **Trap forwarding type** list.
4. Enter a user name in the **User Name** field.
5. (Optional) Enter a context name in the **Context Name** field.
6. Select the authorization protocol in the **Auth Protocol** field.
7. Enter the authorization password in the **Auth Password** field and the **Retype Password** field.
8. Select the privacy protocol in the **Priv Protocol** field.
9. Enter the privacy password in the **Priv Password** field and the **Retype Password** field.
10. Click **Add**.

The **Add/Edit Trap Recipient** dialog box displays.

- a. (Optional) In the **Description** field, enter a description of the trap recipient.
- b. In the **IP Address** field, enter the trap recipient's IP address.

The Management application accepts IP addresses in IPv4 or IPv6 formats.

- c. Enter the trap recipient's UDP port number, in the **port** field.
- d. Click **OK** on the **Add/Edit Trap Recipient** dialog box.

11. Click **OK** on the **SNMP Setup** dialog box.

## Editing a destination

To edit a destination, complete the following steps.

1. Select **Monitor > SNMP Setup**.

The **SNMP Setup** dialog box displays.

2. Click the **Trap Forwarding** tab.

3. Select the destination you want to edit in the **Destinations** table and click **Edit**.

The **Add/Edit Trap Recipient** dialog box displays.

- a. (Optional) In the **Description** field, edit the description of the trap recipient.

- b. In the **IP Address** field, edit the trap recipient's IP address.

The Management application accepts IP addresses in IPv4 or IPv6 formats.

- c. Edit the trap recipient's UDP port number, in the **port** field.

- d. Click **OK** on the **Add/Edit Trap Recipient** dialog box.

4. Click **OK** on the **SNMP Setup** dialog box.

## Removing a destination

To remove a destination, complete the following steps.

1. Select **Monitor > SNMP Setup**.

The **SNMP Setup** dialog box displays.

2. Click the **Trap Forwarding** tab.

3. Select the destination you want to remove in the **Destinations** table and click **Remove**.

Press Ctrl and then click to select more than one destination.

4. Click **OK** on the **SNMP Setup** dialog box.

## Disabling trap forwarding

You can disable trap forwarding on all defined destinations.

To disable trap forwarding, complete the following steps.

1. Select **Monitor > SNMP Setup**.

The **SNMP Setup** dialog box displays.

2. Click the **Trap Forwarding** tab.

3. Clear the **Enable trap forwarding** check box.

4. Click **OK** on the **SNMP Setup** dialog box.

## Enabling SNMP informs

---

**NOTE**

SNMP Informs is only supported on Fabric OS 6.3 or later switches discovered through SNMP v3. For information about discovery through SNMP v3, refer to [“Discovering fabrics”](#) on page 36.

---

You can enable SNMP informs on all Informs-capable Fabric OS switches.

To enable Informs, complete the following steps.

1. Select **Monitor > SNMP Setup**.  
The **SNMP Setup** dialog box displays.
2. Click the **Informs** tab.
3. Select the **Enable informs** option.
4. Select the fabric on which you want to enable Informs from the **Fabric** list.

---

**NOTE**

If you want to enable Informs only on specific switches in a Fabric, you must configure Informs using the Element Manager on each switch or through the command line interface.

---

All Informs-capable switches display in the **SNMP Informs Capable Switch in the Fabric** table.

5. Click **OK** on the **SNMP Setup** dialog box.  
SNMP Informs will be enabled on all switches in the **SNMP Informs Capable Switch in the Fabric** table.

## Disabling SNMP informs

To disable Informs, complete the following steps.

1. Select **Monitor > SNMP Setup**.  
The **SNMP Setup** dialog box displays.
2. Click the **Informs** tab.
3. Select the **Disable informs** option.
4. Select the fabric on which you want to disable Informs from the **Fabric** list.

All Informs-capable switches display in the **SNMP Informs Capable Switch in the Fabric** table.

5. Click **OK** on the **SNMP Setup** dialog box.  
SNMP Informs will be disabled on all switches in the **SNMP Informs Capable Switch in the Fabric** table.

## Syslog forwarding

---

**NOTE**

Syslog messages are only available on Fabric OS devices and Brocade HBAs (managed using HCM Agent).

---

Syslog forwarding is the process by which you can configure the Management application to send Syslog messages to other computers. Switches only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you must configure the Management application to listen on a different port. Then you must configure another Syslog server to listen for Syslog messages and forward the messages to the Management application Syslog listening port. Brocade HBAs only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you the management application cannot send Syslog messages to another computer.

Syslog messages from logical switches are recognized by the WWN of the default switch embedded in the syslog message body. Therefore, to receive syslog messages from logical switches, the associated default switch must also be managed and monitored by the Management application.

Syslog messages are persisted in the database. You can view the Syslog messages from the Management application by selecting **Monitor > Log > Syslog**. You can also view audit syslog messages in the Master Log or by selecting **Monitor > Log > Audit Log**.

### Registering the management server

You can automatically register this server as the Syslog destination on all managed Fabric OS devices.

---

**NOTE**

If the Syslog messages are routed through a relay and the source IP address is not spoofed by the relay before it sends the messages to the Management application, the messages will be dropped.

---

---

**NOTE**

Syslog messages forwarded by the Management application always use the Management server IP address as the source IP address.

---

To register the management server, complete the following steps.

1. Select **Monitor > Syslog Configuration**.  
The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Management Server** tab.
3. Select the **Auto register server as Syslog destination** check box.
4. Enter the Syslog listening port number of the Server in the **Syslog Listening Port (Server)** field.
5. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

## Registering a host server

You can register any host server as the Syslog destination on managed Fabric OS devices. You can register different destinations for different fabrics.

To register a host server, complete the following steps.

1. Select **Monitor > Syslog Configuration**.  
The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Other Destination** tab.
3. Select **Add** from the **Action** list.
4. Enter the IP address of the host server in the **Syslog Destination IP Address** field.
5. Select a fabric from the **Targeted Fabric** list.
6. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

## Removing a host server

You can remove any host server as the Syslog destination on managed Fabric OS devices.

To remove a host server, complete the following steps.

1. Select **Monitor > Syslog Configuration**.  
The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Other Destination** tab.
3. Select **Remove** from the **Action** list.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

## Adding a destination

You can forward Syslog events sent to this server to another destination on a different host.

To add a destination, complete the following steps.

1. Select **Monitor > Syslog Configuration**.  
The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Syslog Forwarding** tab.
3. Click **Add**.  
The **Add/Edit Syslog Recipient** dialog box displays.
  - a. (Optional) In the **Description** field, enter a description of the Syslog recipient.
  - b. In the **IP Address** field, enter the Syslog recipient's IP address.  
The Management application accepts IP addresses in IPv4 or IPv6 formats.
  - c. Enter the Syslog recipient's TCP/IP port number, in the **port** field.
  - d. Click **OK** on the **Add/Edit Syslog Recipient** dialog box.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

## Editing a destination

To edit a destination, complete the following steps.

1. Select **Monitor > Syslog Configuration**.  
The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Syslog Forwarding** tab.
3. Select the destination you want to edit in the **Destinations** table and click **Edit**.  
The **Add/Edit Syslog Recipient** dialog box displays.
  - a. (Optional) In the **Description** field, edit the description of the Syslog recipient.
  - b. In the **IP Address** field, edit the Syslog recipient's IP address.  
The Management application accepts IP addresses in IPv4 or IPv6 formats.
  - c. Edit the Syslog recipient's TCP/IP port number, in the **port** field.
  - d. Click **OK** on the **Add/Edit Syslog Recipient** dialog box.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

## Removing a destination

To remove a destination, complete the following steps.

1. Select **Monitor > Syslog Configuration**.  
The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Syslog Forwarding** tab.
3. Select the destination you want to remove in the **Destinations** table and click **Remove**.  
Press Ctrl and then click to select more than one destination.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

## Enabling Syslog forwarding

You can enable Syslog forwarding on all defined destinations.

To enable trap forwarding, complete the following steps.

1. Select **Monitor > Syslog Configuration**.  
The **Syslog Registration and Forwarding** dialog box displays.
2. Click the **Syslog Forwarding** tab.
3. Select the **Enable Syslog forwarding** check box.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

### Disabling Syslog forwarding

You can disable Syslog forwarding on all defined destinations.

To disable Syslog forwarding, complete the following steps.

1. Select **Monitor > Syslog Configuration**.

The **Syslog Registration and Forwarding** dialog box displays.

2. Click the **Syslog Forwarding** tab.
3. Clear the **Enable Syslog forwarding** check box.
4. Click **OK** on the **Syslog Registration and Forwarding** dialog box.

# Performance Data

---

## In this chapter

• Performance overview.....	287
• Real-time performance data.....	293
• Historical performance data.....	297
• End-to-end monitoring.....	302
• Top Talker monitoring.....	304
• Thresholds and event notification.....	309
• Connection utilization.....	315

## Performance overview

Performance monitoring provides details about the quantity of traffic and errors a specific port or device generates on the fabric over a specific time frame. You can also use performance to indicate the devices that create the most traffic and to identify the ports that are most congested.

Performance allows you to monitor your SAN using the following methods:

- Display the connections which are using the most bandwidth on the selected device or one of the F\_ports on the device with a feature called Top Talkers.
- Gather and display real-time performance data (FC ports, ISL ports, Device ports, GE ports, FCIP tunnels, Managed HBA ports, Managed CNA ports and 10 GE ports).
- Persist and display historical performance data (FC ports, ISL ports, Device ports, FCIP tunnels, and 10 GE ports) for selected fabrics or the entire SAN.
- Support End-to-End monitors for real-time and historical performance data.
- Enforce user-defined performance thresholds and notification when thresholds are exceeded.
- Display percentage utilization for FC and FCIP links.
- Provide aging scheme (5 minutes, 30 minutes, 2 hours and 1 day granularity).
- Provide enhanced performance reports.

## Performance measures

Performance measures enable you to select one or more measures to define the graph or report. The measures available to you depend on the object type from which you want to gather performance data.

- Tx % Utilization — available for FC, GE, Managed HBA ports, Managed CNA ports, 10GE ports, and FCIP tunnels.
- Rx % Utilization — available for FC, GE, Managed HBA ports, Managed CNA ports, 10GE ports, and FCIP tunnels.
- Tx MB/Sec — available for FC and GE, Managed HBA ports, Managed CNA ports, 10GE ports, FCIP tunnels, and End-to-End monitors.
- Rx MB/Sec — available for FC and GE, Managed HBA ports, Managed CNA ports, 10GE ports, FCIP tunnels, and End-to-End monitors.
- CRC Errors — available for FC, Managed HBA ports, Managed CNA ports, 10GE ports and End-to-End monitors.
- Signal Losses — available for Managed HBA ports, Managed CNA ports, and FC ports.
- Sync Losses — available for Managed HBA ports, Managed CNA ports, and FC ports.
- Link Failures — available for Managed HBA ports, Managed CNA ports, and FC ports.
- Sequence Errors — available for FC ports.
- Invalid Transmissions — available for FC ports.
- Rx Link Resets — available for FC ports.
- Tx Link Resets — available for FC ports.
- Dropped Packets — available for FCIP tunnels only.
- Compression Ratio — available for FCIP tunnels only.
- Latency — available for FCIP tunnels only.
- Link Retransmits — available for FCIP tunnels only.
- Timeout Retransmits — available for FCIP tunnels only.
- Fast Retransmits — available for FCIP tunnels only.
- Duplicate Ack Received — available for FCIP tunnels only.
- Window Size RTT — available for FCIP tunnels only.
- TCP Out of Order Segments — available for FCIP tunnels only.
- Slow Start Status — available for FCIP tunnels only.
- Frames Received — available for 10GE ports only.
- Overflow Errors — available for 10GE ports only.
- Runtime Errors — available for 10GE ports only.
- Receive EOF — available for 10GE ports only.
- Too Long Errors — available for 10GE ports only.
- Underflow Errors — available for 10GE ports only.
- Alignment Errors — available for 10GE ports only.
- NOS Count — available for Managed HBA ports and Managed CNA ports.
- Error Frames — available for Managed HBA ports and Managed CNA ports.

- Under Sized Frames — available for Managed HBA ports and Managed CNA ports.
- Over Sized Frames — available for Managed HBA ports and Managed CNA ports.
- Primitive Sequence Protocol Errors — available for Managed HBA ports and Managed CNA ports.
- Dropped Frames — available for Managed HBA ports and Managed CNA ports.
- Bad EOF Frames — available for Managed HBA ports and Managed CNA ports.
- Invalid Ordered Sets — available for Managed HBA ports and Managed CNA ports.
- Non Frame Coding Error — available for Managed HBA ports and Managed CNA ports.

## Performance management requirements

To collect performance data, make sure the following requirements have been met:

- Make sure the snmp access control list for the device is empty or the Management application server IP is in the access control list.

### Example of default access control list

```
FCRRouter:admin> snmpconfig --show accesscontrol
SNMP access list configuration:
Entry 0: No access host configured yet
Entry 1: No access host configured yet
Entry 2: No access host configured yet
Entry 3: No access host configured yet
Entry 4: No access host configured yet
Entry 5: No access host configured yet
```

### Example of Management application Server IP included in access control list

```
FCRRouter:admin> snmpconfig --show accesscontrol
SNMP access list configuration:
Entry 0: Access host subnet area 172.26.1.86 (rw)
Entry 1: No access host configured yet
Entry 2: No access host configured yet
Entry 3: No access host configured yet
Entry 4: No access host configured yet
Entry 5: No access host configured yet
```

To add the Management application server IP address to the access control list, use the `snmpconfig --add accesscontrol` command:

To set the default access control, use the `snmpconfig --default accesscontrol` command:

- Make sure that the SNMP credentials in the Management application match the SNMP credentials on the device.
  - To check the SNMP v1 credentials on the device, use the `snmpconfig --show snmpv1` command.

### Example of SNMP v1

```
HCLSwitch:admin> snmpconfig --show snmpv1
SNMPv1 community and trap recipient configuration:
Community 1: Secret C0de (rw)
Trap recipient: 10.103.4.63
Trap port: 162
Trap recipient Severity level: 4
Community 2: OrigEquipMfr (rw)
```

## 11 Performance management requirements

```
Trap recipient: 10.191.12.240
Trap port: 162
Trap recipient Severity level: 4
Community 3: private (rw)
Trap recipient: 10.103.5.105
Trap port: 162
Trap recipient Severity level: 4
Community 4: public (ro)
Trap recipient: 192.168.102.41
Trap port: 162
Trap recipient Severity level: 4
Community 5: common (ro)
Trap recipient: 10.32.150.116
Trap port: 162
Trap recipient Severity level: 4
Community 6: FibreChannel (ro)
Trap recipient: 1001:0:0:0:0:0:0:172
Trap port: 162
Trap recipient Severity level: 4
```

- To set the SNMP v1 credentials on the device, use the `snmpconfig --set snmpv1` command.

### Example of setting SNMP v1

```
HCLSwitch:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [test]
Trap Recipient's IP address : [172.26.1.183]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [172.26.24.26]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [custom]
Trap Recipient's IP address : [172.26.1.158]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (ro): [custom]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [172.26.1.145]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
```

- To check the SNMP v3 credentials on the device, use the `snmpconfig --show snmpv3` command.

### Example of SNMP v3

```
sw1:FID128:admin> snmpconfig --show snmpv3
SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 2 (rw): snmpadmin2
Auth Protocol: noAuth
```

```

Priv Protocol: noPriv
User 3 (rw): snmpadmin3
Auth Protocol: noAuth
Priv Protocol: noPriv
User 4 (ro): snmpuser1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 5 (ro): snmpuser2
Auth Protocol: noAuth
Priv Protocol: noPriv
User 6 (ro): admin
Auth Protocol: noAuth
Priv Protocol: noPriv

```

- To set the SNMP v3 credentials on the device, use the `snmpconfig --set snmpv3` command.

```

FM_4100_21:admin> snmpconfig --set snmpv3
SNMPv3 user configuration(SNMP users not configured in Fabric OS user
database will have physical AD and admin role as the default):
User (rw): [snmpadmin1] admin
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(1..6) [2] 1
New Priv Passwd:
Verify Priv Passwd:
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]:
(2..2) [2]
SNMPv3 trap recipient configuration:
Trap Recipient's IP address : [192.168.71.32]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [1.1.1.1]
UserIndex: (1..6) [2]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [10.64.209.171]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]

```

## 11 Performance management requirements

```
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
```

- To check SNMP credentials in the Management application, complete the following steps.
  1. Select **Discover > Setup**.  
The **Discover Setup** dialog box displays.
  2. Select an IP address from the **Available Addresses** table.
  3. Click **Edit**.  
The **Address Properties** dialog box displays.
  4. Click the **SNMP** tab.
  5. Select the **v1** or **v3** from the **SNMP Version** list.
  6. Make sure SNMP credentials match those on the device.
  7. Click **OK** on the **Address Properties** dialog box.
  8. Click **Close** on the **Discover Setup** dialog box.
- To set SNMP credentials in the Management application, refer to [“Configuring SNMP credentials”](#) on page 39.
- Make sure that the SNMP security level is set to the appropriate level for the switch.
  - To check the SNMP security level, use the `snmpconfig --show secLevel` command.

### Example of checking SNMP security level

```
snmpconfig --show secLevel
GET security level = 0, SET level = 0
SNMP GET Security Level: No security
SNMP SET Security Level: No security
```

- To set the SNMP security level, use the `snmpconfig --set secLevel` command.
- ### Example of checking SNMP security level
- ```
snmpconfig --set secLevel 0
Select SNMP GET Security Level
(0 = No security, 1 = Authentication only, 2 = Authentication and Privacy,
3 = No Access): (0..3) [0]
```
- To collect performance for GigE ports and FCIP statistics, make sure that SNMP v3 credentials match (see above) and that FCIP-MIB capability is enabled.

- To check FCIP-MIB capability, use the `snmpconfig --show mibcapability` command.

### Example of showing FCIP-MIB

```
FCRRouter:admin> snmpconfig --show mibcapability
FCIP-MIB: YES
```

- To enable FCIP-MIB capability, use the `snmpconfig --set mibcapability` command.

### Example of enabling FCIP-MIB

```
FCRRouter:admin> snmpconfig --set mibcapability
FA-MIB (yes, y, no, n): [yes]
FICON-MIB (yes, y, no, n): [yes]
```

```
HA-MIB (yes, y, no, n): [yes]
FCIP-MIB (yes, y, no, n): [yes]
ISCSI-MIB (yes, y, no, n): [yes]
```

- To collect performance on a Virtual Fabric enabled device, use the `admin> userconfig --show` command to make sure the Fabric OS user has access to all the Virtual Fabrics. Make sure that the SNMPv3 user name is same as the Fabric OS user name. Otherwise, the data is not collected for virtual switches with a non-default VF ID. By default the `admin` user has access to all Virtual Fabrics.

#### Example of Fabric OS user verification

```
swl:FID128:admin> userconfig --show
Account name: admin
Description: Administrator
Enabled: Yes
Password Last Change Date: Unknown
Password Expiration Date: Not Applicable
Locked: No
Home LF Role: admin
Role-LF List: admin: 1-128
Chassis Role: admin
Home LF: 128
```

- Make sure I/O is running on the switch to obtain real statistics. To view switch statistics, use the `portperfshow [slot/]port -[slot/]port | -tx | -rx | -tx -rx | -t <interval> (FC Ports) or portshow fcipunnel <Ge port number> <tunnel no> -perf (FCIP tunnels)` command.

#### Example for FC ports

```
Sprint-65:root> portperfshow 5
```

#### Example for FCIP tunnels

```
Sprint-65:root> portshow fcipunnel ge0 1 -perf
```

## Real-time performance data

Real-time performance enables you to collect data from managed devices in your SAN. Real-time performance is only supported on the following managed objects: FC (E\_ and F\_ports), GE\_ports, 10GE\_ports, Managed HBA Ports, Managed CNA Ports, and FCIP tunnels. You can use real-time performance to configure the following options:

- Select the polling rate from 10 seconds up to 1 minute.
- Select up to 32 ports total from a maximum of 10 devices for graphing performance.

---

#### NOTE

Virtual Fabric logical ISL ports are not included in performance collection.

---

- Choose to display the same Y-axis range for both the Tx MB/Sec and Rx MB/Sec measure types for easier comparison of graphs.

## Generating a real-time performance graph

You can monitor a device's performance through a performance graph that displays transmit and receive data. The graphs can be sorted by the column headers. You can create multiple real-time performance graph instances.

### NOTE

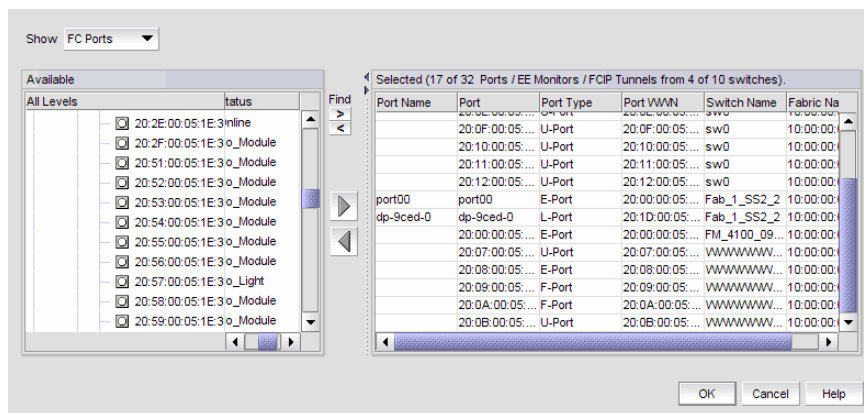
To make sure that statistic collection for a switch does not fail, you must configure SNMP credentials for the switch. For step-by-step instructions, refer to [“Configuring SNMP credentials”](#) on page 39.

To generate a real-time performance graph for a device, complete the following steps.

1. Select the fabric, device, or port for which you want to generate a performance graph.
2. Choose one of the following options:
  - Select **Monitor > Performance > Real-Time Graph**.
  - OR
  - Right-click the device or fabric and select **Performance > Real-Time Graph**.

If you selected a port, the **Real Time Performance Graphs** dialog box for the selected port displays. To filter real-time performance data from the **Real Time Performance Graphs** dialog box, refer to [“Filtering real-time performance data”](#) on page 295.

If you selected a fabric or device, the **Realtime Port Selector** dialog box displays. Continue with [step 3](#).



**FIGURE 107** Realtime Port Selector dialog box

3. Select the object type (FC Ports, ISL Ports, Device Ports, EE Monitors, GE Ports, FCIP Tunnels, Managed HBA Ports, Managed CNA Ports, or 10GE Ports) by which you want to graph performance from the **Show** list.
4. Right-click anywhere in the **Available** table and select **Expand All**.
5. Select the ports you want to include in the performance graph in the **Available** table. Press **Ctrl** or **Shift** and then click to select more than one port.
6. Click the right arrow to move the selected ports to the **Selected** table.
7. Click **OK**.

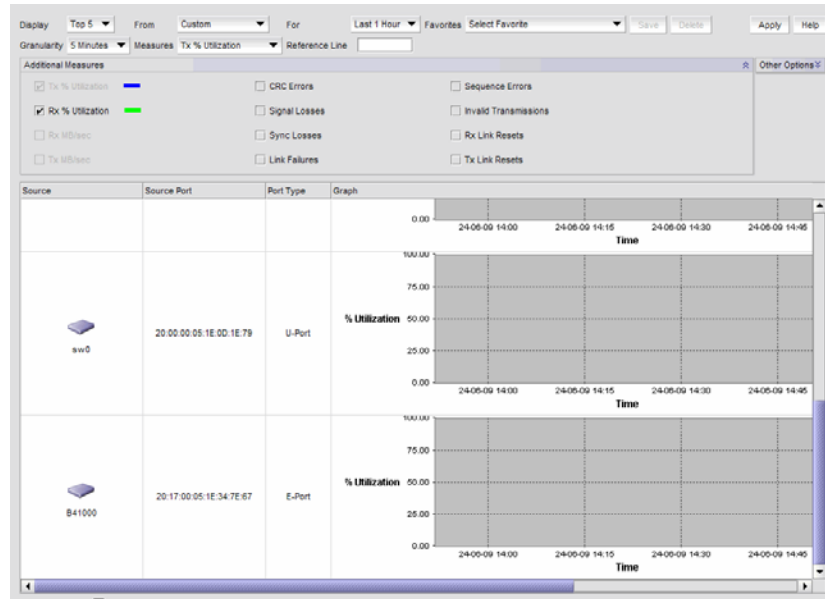
The **Real Time Performance Graphs** dialog box displays.

## Filtering real-time performance data

To filter real-time performance data from the **Real Time Performance Graphs** dialog box, complete the following steps.

1. Open the **Real Time Performance Graphs** dialog box.

For step-by-step instructions, refer to [“Generating a real-time performance graph”](#) on page 294. The **Real Time Performance Graphs** dialog box displays.



**FIGURE 108** Real Time Performance Graphs dialog box

2. Click **Select** to change the object type.
3. Select the object type (FC Ports, ISL Ports, Device Ports, EE Monitors, GE Ports, FCIP Tunnels, Managed HBA Ports, Managed CNA Ports, or 10GE Ports) by which you want to graph performance from the **Show** list.
4. Right-click anywhere in the **Available** table and select **Expand All**.
5. Select the ports you want to include in the performance graph in the **Available** table.  
Press **Ctrl** or **Shift** and then click to select more than one port.

6. Click the right arrow to move the selected ports to the **Selected** table.
7. Click **OK**.

The **Real Time Performance Graphs** dialog box displays.

8. Select the measure by which you want to gather performance data from the **Measures** list.  
To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.
9. (Optional) Enter a value (percentage) in the **Reference Line** field to set a reference for the transmit and receive utilization.

Note that this field is only available when you select **Tx % Utilization** or **Rx % Utilization** from the **Measures** list.

## 11 Exporting real-time performance data

10. Select the granularity at which you want to gather performance data from the **Granularity** list.
11. Select the **Interpolate** check box to use interpolation to fill existing gaps, if necessary.
12. (Optional) Click **Other Options** and select the **Use Same Y-axis** check box to make the Y-axis range the same for object.

The **Use Same Y-axis** check box is only available when you select **Rx MB/sec** and **Tx MB/sec** from the **Measures** list. You do not have to apply this change, the performance graph automatically updates.

13. Move the **Row Height** slider to the left to make the row height smaller or to the right to make it bigger.
14. Select the **Display tabular data only** check box to only show text with no graphs or icons.  
The **Source** and **Destination** icons and the **Graph** column do not display
15. Click **Apply**.

The selected graph automatically displays in the **Real Time Performance Graphs** dialog box.

16. Click the close button (X) to close the **Real Time Performance Graphs** dialog box.

### Exporting real-time performance data

To export real-time performance data, complete the following steps.

1. Generate a performance graph.  
To generate a performance graph, refer to [“Generating a real-time performance graph”](#) on page 294.
2. Right-click anywhere in the graph table and select **Export Table**.  
The **Save table to a tab delimited file** dialog box displays.
3. Browse to the file location where you want to save the performance data.
4. Enter a name for the file and click **Save**.

### Clearing port counters

To reset all port statistic counters to zero on a selected device, complete the following steps.

1. Right-click a device on the Connectivity Map or Product List and select **Performance > Clear Counters**.
2. Click **Yes** on the message.  
A **Port Stats Counter Reset** message displays. If any of the counters do not clear, the message displays a list of the associated ports.
3. Click **Ok** on the **Port Stats Counter Reset** message.



## 11 Disabling historical performance collection

2. Select the fabrics for which you want to collect historical performance data in the **Available** table.
3. Click the right arrow to move the selected fabrics to the **Selected** table.
4. Select the **Include newly discovered fabrics** check box to automatically add all newly discovered fabrics to the **Selected** table.
5. Click **OK**.

Historical performance data collection is enabled for all selected fabrics.

### Disabling historical performance collection

To disable historical performance collection on all fabrics, select **Monitor > Performance > Historical Data Collection > Disable All**.

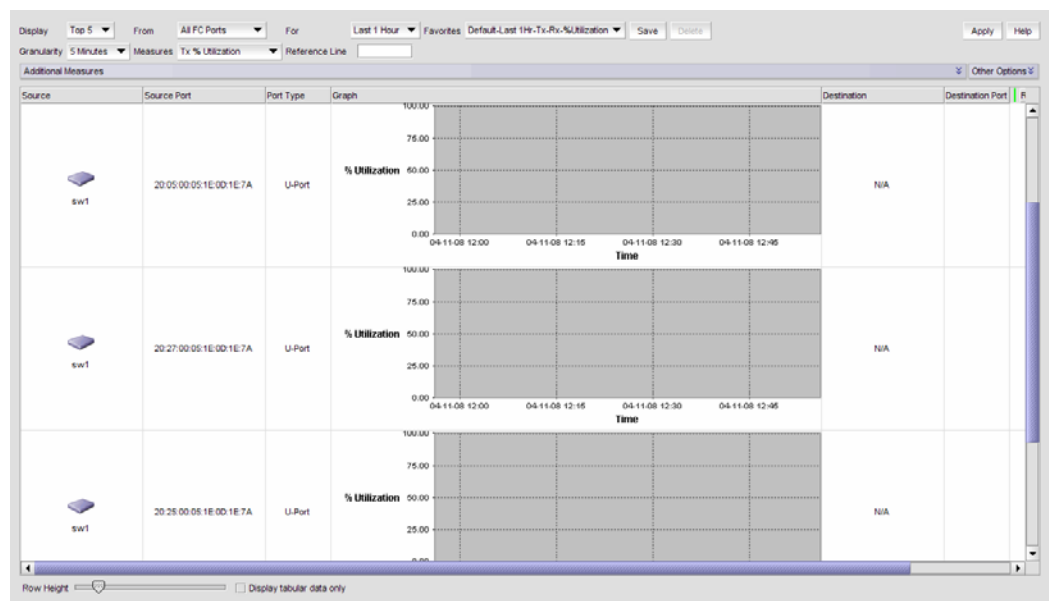
Historical performance data collection is disabled for all fabrics in the SAN.

### Generating a historical performance graph

To generate a historical performance graph for a device, complete the following steps.

1. Select the device for which you want to generate a performance graph.
2. Choose one of the following options:
  - Select **Monitor > Performance > Historical Graph**.
  - OR
  - Right-click the device or fabric and select **Performance > Historical Graph**.

The **Historical Performance Graph** dialog box displays.



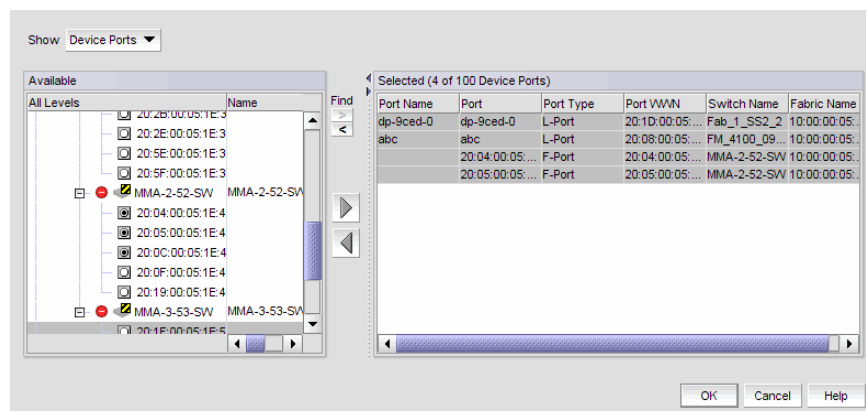
**FIGURE 110** Historical Performance Graphs dialog box

3. Select a default from the **Favorites** list or filter the historical data by completing the following steps.
  - a. Select the number of results to display from the **Display** list.
  - b. Select the ports from which you want to gather performance data from the **From** list.  
If you select **Custom**, refer to [“Filtering data by ports”](#) on page 299.
  - c. Select the historical period for which you want to gather performance data from the **For** list.  
If you select **Custom**, refer to [“Filtering data by time”](#) on page 300.
  - d. Select the granularity at which you want to gather performance data from the **Granularity** list.
  - e. Select the measure by which you want to gather performance data from the **Measures** list.  
To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.
  - f. Move the **Row Height** slider to the left to make the row height smaller or to the right to make it bigger.
  - g. Select the **Display tabular data only** check box to only show text with no graphs or icons.  
The **Source** and **Destination** icons and the **Graph** column do not display.
  - h. Click **Apply**.  
The selected graph automatically displays in the **Historical Performance Graph** dialog box.  
To save a filtered graph, refer to [“Saving a historical performance graph configuration”](#) on page 300.  
To delete user-defined graph, refer to [“Deleting a historical performance graph”](#) on page 301.
4. Click the close button (X) to close the **Historical Performance Graph** dialog box.

### *Filtering data by ports*

To filter data for a historical performance graph by ports, complete the following steps.

1. Select the type of ports from the **Show** list.



**FIGURE 111** Custom Port Selector dialog box

## 11 Saving a historical performance graph configuration

2. Right-click a device in the **Available** table and select **Expand All**.
3. Select the ports (press **Ctrl** or **Shift** and then click to select multiple ports) from which you want to gather performance data from the **Available** table and click the right arrow button.

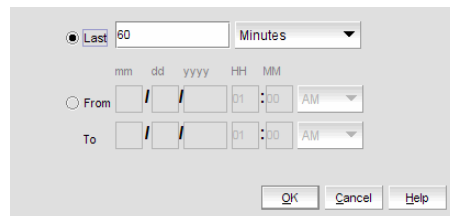
The selected ports move to the **Select Ports** table.

4. Click **OK**.

### *Filtering data by time*

To filter data for a historical performance graph by time, complete the following steps.

1. Select the **Last** option and enter the number of minutes, hours, or days.  
OR  
Select the **From** option and enter the date and time.

The image shows a dialog box titled "Custom Port Selector". It has two radio buttons: "Last" (selected) and "From". The "Last" option has a text input field containing "60" and a dropdown menu set to "Minutes". The "From" option has a date and time picker with fields for month (mm), day (dd), year (yyyy), hour (HH), minute (MM), and AM/PM. Below the "From" option is a "To" field with similar date and time picker components. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

**FIGURE 112** Custom Port Selector dialog box

2. Click **OK**.

## Saving a historical performance graph configuration

To save a historical performance graph configuration, complete the following steps.

1. Select the device for which you want to generate a performance graph.
2. Choose one of the following options:
  - Select **Monitor > Performance > Historical Graph**.
  - OR
  - Right-click the device or fabric and select **Performance > Historical Graph**.

The **Historical Performance Graph** dialog box displays.

3. Filter the historical data by completing the following steps.
4. Select the number of results to display from the **Display** list.
5. Select the ports from which you want to gather performance data from the **From** list.  
If you select **Custom**, you can not save the configuration.
6. Select the historical period for which you want to gather performance data from the **For** list.  
If you select **Custom**, you can not save the configuration.
7. Select the granularity at which you want to gather performance data from the **Granularity** list.
8. Select the measure by which you want to gather performance data from the **Measures** list.

To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.

9. Enter a reference line value percentage for Tx% or Rx % Utilization.  
This field is only enabled when Tx% or Rx % Utilization is selected from the **Measures** list.
10. Move the **Row Height** slider to the left to make the row height smaller or to the right to make it bigger.
11. Select the **Display tabular data only** check box to only show text with no graphs or icons.  
The **Source** and **Destination** icons and the **Graph** column do not display
12. Save this configuration by selecting **Save**.  
The **Save Favorites** dialog box displays. This enables you to save the selected configuration so that you can use it to generate the same type of report at a later date.
13. Enter a name for the configuration in the **Favorites Name** field.
14. Click **OK**.
15. Click **Apply**.  
The selected graph automatically displays in the **Historical Performance Graph** dialog box.
16. Click the close button (X) to close the **Historical Performance Graph** dialog box.

## Exporting historical performance data

To export historical performance data, complete the following steps.

1. Generate a performance graph.  
To generate a performance graph, refer to [“Generating a historical performance graph”](#) on page 298.
2. Right-click anywhere in the graph table and select **Export Table**.  
The **Save table to a tab delimited file** dialog box displays.
3. Browse to the file location where you want to save the performance data.
4. Enter a name for the file and click **Save**.

## Deleting a historical performance graph

To delete a user-defined historical performance graph configuration, complete the following steps.

1. Select the device for which you want to generate a performance graph.
2. Choose one of the following options:
  - Select **Monitor > Performance > Historical Graph**.
  - OR
  - Right-click the device or fabric and select **Performance > Historical Graph**.

The **Historical Performance Graph** dialog box displays.

3. Select the configuration you want to delete from the **Favorites** list.

You can only delete a user-defined historical performance graph. You cannot delete a default favorite historical performance graph.

4. Click **Delete**.
5. Click **Yes** on the confirmation message.
6. Click the close button (X) to close the **Historical Performance Graph** dialog box.

## End-to-end monitoring

### NOTE

End-to-end monitoring requires a Fabric OS device.

Performance enables you to provision end-to-end monitors of selected target and initiator pairs. These monitors are persisted in the database and are enabled on one of the F\_ports on the connected device (the Management application server determines the port). You can use these monitors to view both real-time and historical performance data.

### NOTE

A Top Talker and an end-to-end monitor cannot be configured on the same fabric. You must delete the Top Talker monitor before you configure the end-to-end monitor.

## Configuring an end-to-end monitor pair

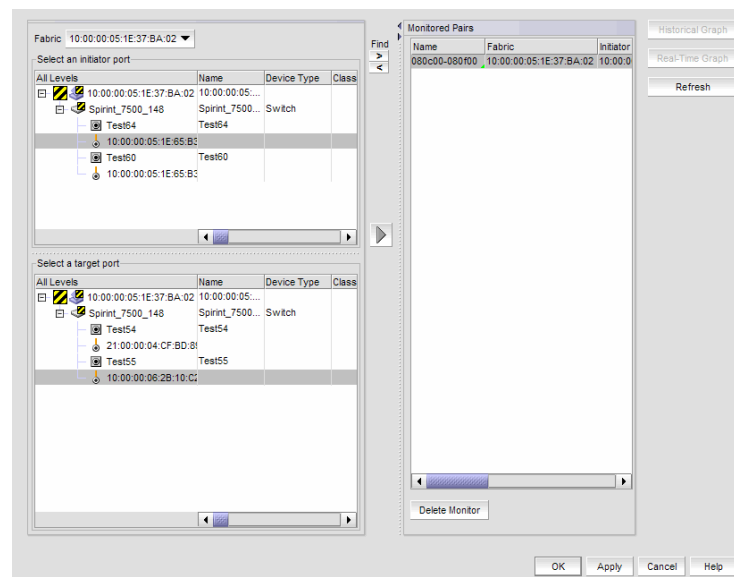
### NOTE

Either the initiator device or the target device must have a Performance Monitor license configured to create an end-to-end monitor.

To configure an end-to-end monitor pair, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors**.

The **Set End-to-End Monitors** dialog box displays.



**FIGURE 113** Set End-to-End Monitors dialog box

2. Select the fabric for which you want to configure end-to-end monitoring from the **Fabric** list.
3. Select an initiator port from the **Select an initiator port** table.
4. Select a target port from the **Select a target port** table.
5. Click the right arrow to move the selected initiator and target ports to the **Monitored Pairs** table.

The system automatically determines the initiator SID and the target DID identifiers for the pair and displays them in the **Monitored Pairs** table.

6. Click **Apply**.

Once the end-to-end monitored pair is applied to the device, the **Status** column in the **Monitored Pairs** table displays 'Enabled'.

---

#### NOTE

If the initiator or target port is part of a logical switch and you move it to another logical switch, the end-to-end monitor fails.

---

Once you have created the end-to-end monitored pair, you can view both real-time and historical performance data. For step-by-step instructions refer to [“Displaying end-to-end monitor pairs in a real-time graph”](#) on page 303 or [“Displaying end-to-end monitor pairs in a historical graph”](#) on page 303.

## Displaying end-to-end monitor pairs in a real-time graph

To display an end-to-end monitor pair in a graph, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors**.  
The **Set End-to-End Monitor** dialog box displays.
2. Select one or more end-to-end monitor pairs you want to view from the **Monitored Pairs** table.  
You can select up to 32 monitored pairs.
3. Click **Real-Time Graph**.  
The **Real Time Performance Graphs** dialog box displays.

## Displaying end-to-end monitor pairs in a historical graph

To display monitored pairs in a historical graph, data collection must be enabled for the selected fabric or enabled SAN wide.

To display an end-to-end monitor pair in a graph, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors**.  
The **Set End-to-End Monitor** dialog box displays.
2. Select one or more end-to-end monitor pairs you want to view from the **Monitored Pairs** table.  
You can select up to 100 monitored pairs.
3. Click **Historical Graph**.  
The **Historical Performance Graph** dialog box displays.

### Refreshing end-to-end monitor pairs

The Management application enables you to rewrite the end-to-end monitors (deleted through CLI or an Element Manager) back to a device.

To refresh all end-to-end monitor pairs, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors**.

The **Set End-to-End Monitor** dialog box displays.

2. Click **Refresh**.

All end-to-end monitor pairs are rewritten back to any devices where the end-to-end monitor pairs were deleted through CLI or an Element Manager.

3. Click **OK**.

### Deleting an end-to-end monitor pair

To delete an end-to-end monitor pair, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors**.

The **Set End-to-End Monitor** dialog box displays.

2. Select the end-to-end monitor pair you want to delete from the **Monitored Pairs** table.

3. Click **Delete Monitor**.

4. Click **OK**.

## Top Talker monitoring

---

#### NOTE

Top Talkers requires the Advance Performance Monitoring (APM) license on the device.

---

---

#### NOTE

Top Talkers requires Fabric OS version 6.2 or later.

---

---

#### NOTE

On the 24 - 8 Gbps FC Port, 8 - 10 Gbps CEE Port Switch, Top Talkers is only supported on the 8 Gbps FC Ports.

---

Advanced Performance Monitoring enables you to create Top Talker monitors on selected devices. Use Top Talkers to display the connections which are using the most bandwidth on the selected device or port. Top Talkers can be enabled on the device or one of the F\_ports on the device. You can only use Top Talkers to view real-time performance data. Data is only collected while the **Top Talkers** dialog box is open; it is not persisted in the database.

You can have multiple Top Talker monitors configured at the same time. You can monitor up to 10 switches for Fabric mode Top Talkers and 32 ports and 10 switches for F\_Port Top Talkers; however, you can only monitor one device or port for each Top Talker you configure.

## Configuring a fabric mode Top Talker monitor

### NOTE

A fabric mode Top Talker and an end-to-end monitor cannot be configured on the same fabric. You must delete the end-to-end monitor before you configure the fabric mode Top Talker.

### NOTE

A fabric mode Top Talker and an F\_port mode Top Talker cannot be configured on the same fabric. You must delete the F\_port mode Top Talker before you configure the fabric mode Top Talker.

To configure a fabric mode Top Talker monitor, complete the following steps.

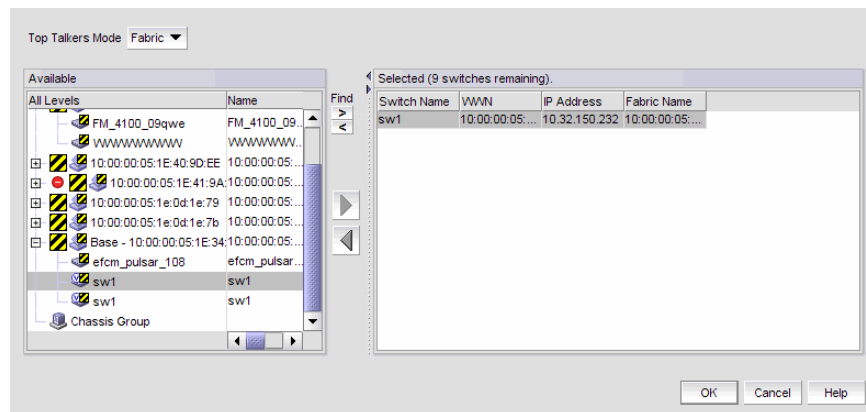
1. Select the device or fabric on which you want to monitor Top Talker data.

### NOTE

On the 24 - 8 Gbps FC Port, 8 - 10 Gbps CEE Port Switch, Top Talkers is only supported on the 8 Gbps FC Ports.

2. Select **Monitor > Performance > Top Talkers**.

The **Top talker Selector** dialog box displays.



**FIGURE 114** Top talker Selector dialog box

3. Select **Fabric** to select a switch to monitor in the **Top Talker Mode** list.

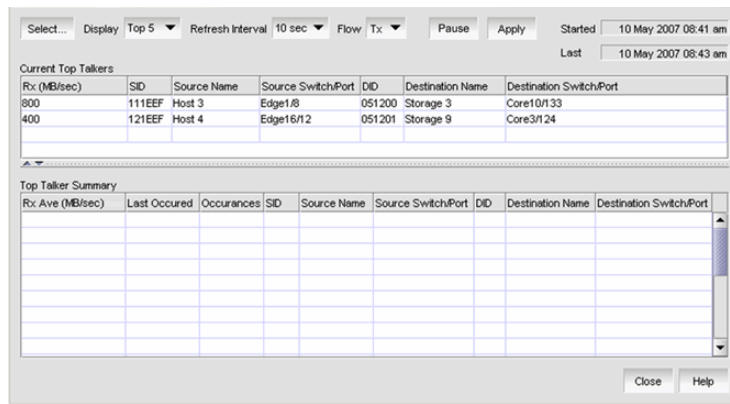
You can only select one device on which to enable Top Talker.

4. Click **OK** on the **Top talker Selector** dialog box.

Top Talker is enabled on the selected device. The **Top Talkers - Fabric Mode for Device\_Name** dialog box displays.

The **Top Talkers - Fabric Mode for Device\_Name** dialog box displays.

## 11 Configuring a fabric mode Top Talker monitor



**FIGURE 115** Top Talkers dialog box

5. Select the number of Top Talkers (1 through 20) to display from the **Display** list.
6. Select how often you want the Top Talker to refresh (10, 20, 30, 40, or 50 seconds, or 1 minute) from the **Refresh Interval** list.
7. Click **Apply**.

The top 20 conversations display in the **Current Top Talkers** table. The **Top Talkers Summary** table displays all Top Talkers that occurred since the **Top Talkers** dialog box was opened (displays a maximum of 360). When the maximum is reached, the oldest Top Talker drops as a new one occurs.

The fabric mode Top Talker provides the following details:

- Tx+Rx Ave (MB/sec)
- Occurrences
- Source
- Source Switch/Port
- Destination
- Destination Switch/Port
- Last Occurred
- SID
- Source Port
- DID
- Destination Port

8. Click the minimize button to hide this dialog box when it is not needed.

## Configuring an F\_port mode Top Talker monitor

---

### NOTE

An F\_port mode Top Talker and an end-to-end monitor cannot be configured on the same F\_port. You must delete the end-to-end monitor before you configure the F\_port mode Top Talker.

---



---

### NOTE

An F\_port mode Top Talker and a fabric mode Top Talker cannot be configured on the same fabric. You must delete the fabric mode Top Talker before you configure the F\_port mode Top Talker.

---

To configure an F\_port mode Top Talker monitor, complete the following steps.

1. Select the port on which you want to monitor Top Talker data.

2. Select **Monitor > Performance > Top Talkers**.

The **Top Talkers - F Port Mode for F\_Port** dialog box displays.

3. Click **Select**.

The **Top talker Selector** dialog box displays.

4. Select **F Port** to select the F\_port to monitor in the **Top Talker Mode** list.

You can only select one F\_port on which to enable the Top Talker monitor.

5. Click **OK** on the **Top Talker Selector** dialog box.

Top Talker is enabled on the selected port.

6. Select the number of Top Talkers (1 through 20) to display from the **Display** list.

7. Select how often you want the Top Talker to refresh (10, 20, 30, 40, or 50 seconds, or 1 minute) from the **Refresh Interval** list.

8. Select whether you want to monitor the receive (Rx) flow or the transmit (Tx) flow for the port from the **Flow** list.

9. Click **Apply**.

The top 20 conversations display in the **Current Top Talkers** table. The **Top Talkers Summary** table displays all Top Talkers that occurred since the **Top Talkers** dialog box was opened (displays a maximum of 360). When the maximum is reached, the oldest Top Talker drops as a new one occurs.

The F\_port mode Top Talker provides the following details:

- |                                      |                    |
|--------------------------------------|--------------------|
| • Rx Ave (MB/sec) or Tx Ave (MB/sec) | • Last Occurred    |
| • Occurrences                        | • SID              |
| • Source                             | • Source Port      |
| • Source Switch/Port                 | • DID              |
| • Destination                        | • Destination Port |
| • Destination Switch/Port            | • Port Speed       |
| • % Utilization                      |                    |

10. Click the minimize button to hide this dialog box when it is not needed.

### Deleting a Top Talker monitor

To delete a Top Talker monitor, complete the following steps.

1. Select the dialog box of the Top Talker monitor you want to delete.
2. Click **Close**.
3. Click **Yes** on the 'do you want to delete this monitor' message.

### Pausing a Top Talker monitor

To pause a Top Talker monitor, complete the following steps.

1. Select the dialog box of the Top Talker monitor you want to pause.
2. Click **Pause**.

### Restarting a Top Talker monitor

To restart a Top Talker monitor, complete the following steps.

1. Select the dialog box of the Top Talker monitor you want to restart.
2. Click **Continue**.

## Thresholds and event notification

Performance allows you to apply thresholds and event notification to real-time performance data. A performance monitor process (thread) monitors the performance data against the threshold setting for each port and issues an appropriate alert to notify you when the threshold is exceeded. For information about configuring event notification, refer to *Event Notification*.

### NOTE

It is not necessary to configure event notification to receive events in the master log. If the threshold is exceeded for a threshold, an event is automatically generated and displayed in the master log.

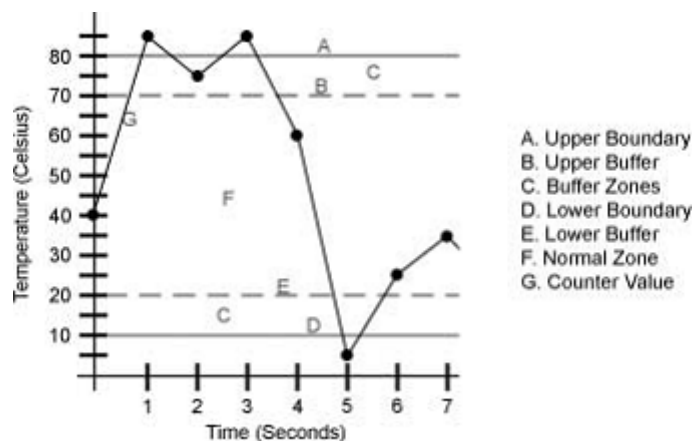
## Creating a threshold policy

### NOTE

If you set the threshold for a particular critical event to 100%, by the time you are notified, it may be too late to prevent a failure. However, when you set the threshold to 85%, for example, you may be able to prevent the failure from occurring.

### Example

The values at 1 second, 3 seconds, and 5 seconds generate events because they exceed boundaries. The value at 2 seconds does not generate an event because, although it crosses the boundary, it remains in the buffer zone. The value at 6 seconds generates an event because it crosses the lower boundary and returns to a value beyond the buffer zone.



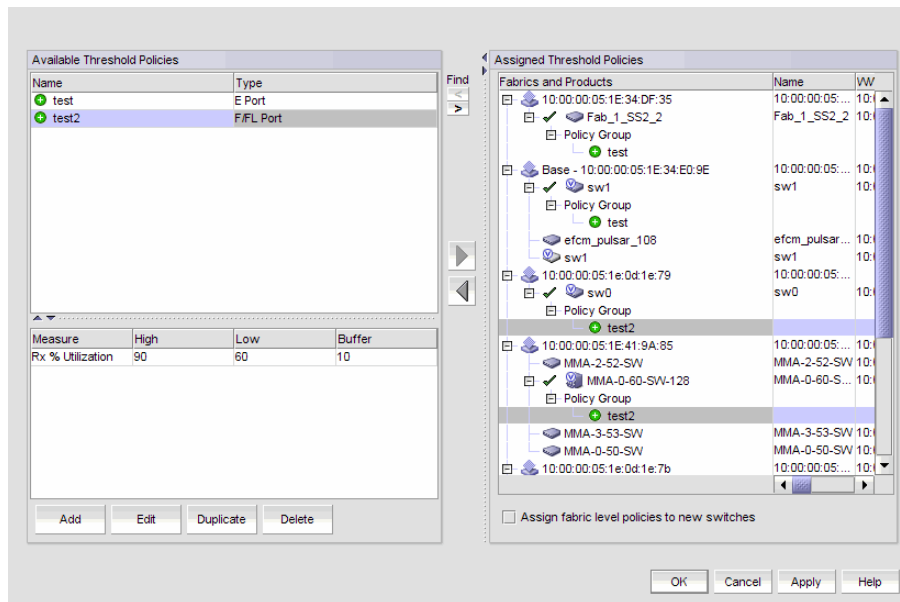
**FIGURE 116** Threshold example

To create a threshold policy, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds**.

The **Set Threshold Policies** dialog box displays.

# 11 Creating a threshold policy



**FIGURE 117** Set Threshold Policies dialog box

2. Click **Add**.

The **New Threshold Policy** dialog box displays.

**FIGURE 118** New Threshold Policy dialog box

3. Enter a name for the policy (100 characters maximum) in the **Name** field.
4. Select a policy type from the **Policy Type** list.


You can only define policies for E and F/FL ports.

5. Select a measure from the **Measure** list.

You can only define policies for the Tx and Rx % Utilization measures. You cannot add the same measure more than once. If you try to add another threshold with the same measure, the new values overwrite the older threshold values in the **Selected Thresholds** table.

6. Enter a percentage for the high boundary in the **High Boundary** field.

When the counter value exceeds high boundary, an event is raised.

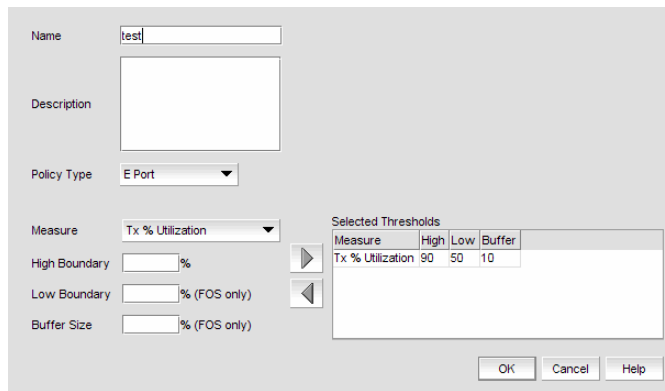
7. (Fabric OS only) Enter a percentage for the low boundary in the **Low Boundary** field.  
When the counter value goes below the low boundary an event is raised.
8. (Fabric OS only) Enter a percentage for the buffer in the **Buffer Size** field.  
Counters may fluctuate around the upper or lower boundary of a range threshold, and as a result cause numerous events in a short period of time. To reduce the number of events, configure a buffer (a range of values just below the upper boundary and just above the lower boundary) in which a counter does not register an event if it returns to a “normal” value. An event only registers if the counter returns to a “normal” value beyond the buffer.
9. Click the right arrow button to move the threshold to the **Selected Thresholds** table.  
If an error is detected, a message displays informing you to enter a valid value. Click **OK** to close this message. Fix any errors and repeat step 9.
10. Repeat steps 5 through 9 for each measure that you want to add to the policy.
11. Click **OK** on the **New Threshold Policy** dialog box.  
The threshold policy displays in the **Available Threshold Policies** table with an added icon (  ).  
To assign a threshold policy to a fabric or device, refer to [“Assigning a threshold policy”](#) on page 313.
12. Click **OK** on the **Set Threshold Policies** dialog box.  
The **Confirm Threshold Changes** dialog box displays.
13. Make the threshold changes by selecting one of the following options:
  - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
  - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.
14. Click **OK** on the **Confirm Threshold Changes** dialog box.

## Editing a threshold policy

To edit a threshold policy, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds**.  
The **Set Threshold Policies** dialog box displays.
2. Select the threshold policy you want to edit in the **Available Threshold Policies** table.
3. Click **Edit**.  
The **Edit Threshold Policy** dialog box displays.

## 11 Editing a threshold policy



The dialog box for editing a threshold policy. It includes fields for Name, Description, Policy Type, Measure, High Boundary, Low Boundary, and Buffer Size. A table titled 'Selected Thresholds' shows the current configuration.

| Measure          | High | Low | Buffer |
|------------------|------|-----|--------|
| Tx % Utilization | 90   | 50  | 10     |

**FIGURE 119** Edit Threshold Policy dialog box

4. Change the policy type from the **Policy Type** list.
5. Select a measure from the **Measure** list.

You cannot add the same measure more than once. If you try to add another threshold with the same measure, the new values overwrite the older threshold values in the **Selected Thresholds** table.

6. Enter a percentage for the high boundary in the **High Boundary** field.
7. (Fabric OS only) Enter a percentage for the low boundary in the **Low Boundary** field.
8. (Fabric OS only) Enter a percentage for the buffer in the **Buffer Size** field.
9. Click the right arrow button to move the threshold to the **Selected Thresholds** table.

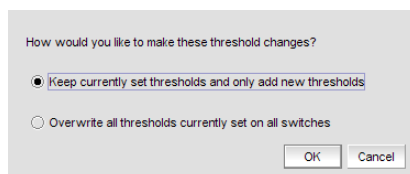
If an error is detected, a message displays informing you to enter a valid value. Click **OK** to close this message. Fix any errors and repeat step 9.

10. Repeat steps 5 through 9 for each measure that you want to add to the policy.
11. Click **OK** on the **Edit Threshold Policy** dialog box.

The threshold policy displays in the **Available Threshold Policies** table with a modified icon ( ). To assign a threshold policy to a fabric or device, refer to [“Assigning a threshold policy”](#) on page 313.

12. Click **OK** on the **Set Threshold Policies** dialog box.

The **Confirm Threshold Changes** dialog box displays.




The dialog box for confirming threshold changes. It asks 'How would you like to make these threshold changes?' and provides two options: 'Keep currently set thresholds and only add new thresholds' (selected) and 'Overwrite all thresholds currently set on all switches'.

**FIGURE 120** Confirm Threshold Changes dialog box

13. Make the threshold changes by selecting one of the following options:
  - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
  - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.
14. Click **OK** on the **Confirm Threshold Changes** dialog box.

## Duplicating a threshold policy

To duplicate a threshold policy, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds**.  
The **Set Threshold Policies** dialog box displays.
2. Select the threshold policy you want to copy in the **Available Threshold Policies** table.
3. Click **Duplicate**.  
The threshold policy displays in the **Available Threshold Policies** table with an added icon (  ) using the following naming format copy of *Threshold\_Name*. To edit the threshold, refer to [“Editing a threshold policy”](#) on page 311. To assign a threshold policy to a fabric or device, refer to [“Assigning a threshold policy”](#) on page 313.
4. Click **OK** on the **Set Threshold Policies** dialog box.  
The **Confirm Threshold Changes** dialog box displays.
5. Make the threshold changes by selecting one of the following options:
  - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
  - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.
6. Click **OK** on the **Confirm Threshold Changes** dialog box.

## Assigning a threshold policy

To assign a threshold policy to a fabric or device, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds**.  
The **Set Threshold Policies** dialog box displays.
2. Select one or more threshold policies you want to assign to a fabric or device in the **Available Threshold Policies** table.  
Press **Ctrl** or **Shift** and then click to select multiple policies.

## 11 Deleting a threshold policy

3. Select one or more fabrics or devices to which you want to assign the policy in the **Available Threshold Policies** table.

If you choose to assign the policy to a fabric and a M-EOS logical switch is present in the fabric, the policy is not assigned to the M-EOS logical switch. You must directly assign a policy to a M-EOS physical chassis.

When you directly assign a policy to a M-EOS physical chassis, the policy is assigned to all logical switches in the physical chassis.

Press **Ctrl** or **Shift** and then click to select multiple fabrics or devices.

4. Click the right arrow button to apply the selected policies to the selected fabrics and devices.

If any of the selected devices do not have a Fabric Watch license, the threshold policies are not set on the device and a message displays listing the affected devices. You will need to upgrade the Fabric Watch license and then assign threshold policies to these devices. Click **OK** to close the message.

5. Click **OK** on the **Set Threshold Policies** dialog box.

The **Confirm Threshold Changes** dialog box displays.

6. Make the threshold changes by selecting one of the following options:

- To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
- To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.

7. Click **OK** on the **Confirm Threshold Changes** dialog box.

### Deleting a threshold policy

To delete a threshold policy, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds**.

The **Set Threshold Policies** dialog box displays.

2. Select the threshold policy you want to delete in the **Available Threshold Policies** table.

When you delete a policy from the M-EOS physical chassis, the policy is deleted from all logical switches in the physical chassis.

3. Click **Delete**.

The threshold policy displays in the **Available Threshold Policies** table with a removed icon (  ).

4. Click **Yes** on the confirmation message.

5. Click **OK** on the **Set Threshold Policies** dialog box.

The **Confirm Threshold Changes** dialog box displays.

6. Make the threshold changes by selecting one of the following options:
  - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
  - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.
7. Click **OK** on the **Confirm Threshold Changes** dialog box.

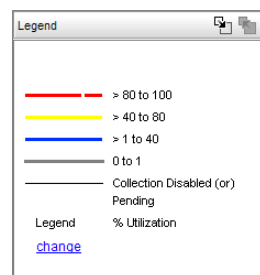
## Connection utilization

### NOTE

Connection utilization is only supported on the following managed objects: E\_ports, F\_ports, N\_ports, 10 GE\_ports and FCIP tunnels.

Performance connection utilization for device ports provides the following features:

- Turns the utilization display on and off from the menu and tool bar.
- Displays moving dotted colored lines that originate from a port.
- Displays two lines in the topology (when turned on); one represents percentage utilization for transmit and the other percentage utilization for receive. The movement of the line determines if it is a transmit or a receive.
  - Receive (Rx)—line moves into a port.
  - Transmit (Tx)—line moves out of a port.
- Displays different colors to represent the percentage utilization range ([Figure 121](#)).



**FIGURE 121** Utilization Legend

The colors and their meanings are outlined in the following table.


| Line Color  | Utilization Defaults    |
|-------------|-------------------------|
| Red line    | 80% to 100% utilization |
| Yellow line | 40% to 80% utilization  |
| Blue line   | 1% to 40% utilization   |
| Gray line   | 0% to 1% utilization    |
| Black line  | Utilization disabled    |

## Enabling connection utilization

### NOTE

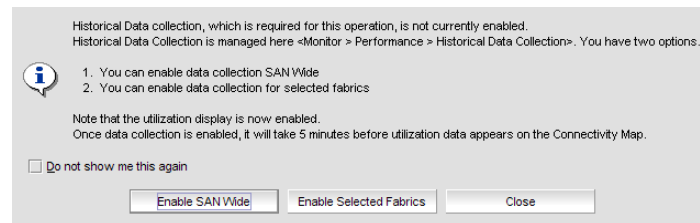
Fabrics where performance data collection is not enabled display connections as thin black lines.

To display the connection utilization, complete the following steps.

1. Choose from one of the following options:
  - Select **Monitor > Performance > View Utilization**
  - Press CTRL + U.
  - Click the Utilization icon (  ).

If you have already enabled historical data collection, the Utilization Legend displays in the main interface window.

If you have not already enabled historical data collection, a message appears informing you that you must enable historical data collection before you can view utilization.



**FIGURE 122** Historical Data Collection message

2. Choose one of the following options:
  - Select **Enable SAN Wide** to enable data collection for the entire SAN.
  - Select **Enable Selected Fabrics** to enable data collection for specific fabrics.

The Historical Data Collection dialog box displays. To select the fabrics on which you want to enable data collection, refer to [“Enabling historical performance collection for selected fabrics”](#) on page 297.

If you click **Close** on the Historical Data Collection message, Historical Data Collection is not enabled; however, the Utilization Legend still displays in the main window.


There is a 5 minute delay to start displaying values.

## Disabling connection utilization

### NOTE

Fabrics where performance data collection is not enabled display connections as thin black lines.

To turn off the connection utilization, choose one of the following options:

- Select **Monitor > Performance > View Utilization** (or CTRL + U).
- Press CTRL + U.
- Click the Utilization icon (  ).

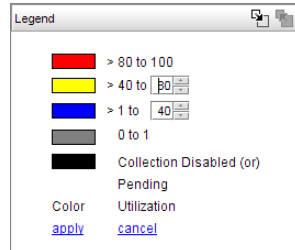
The Utilization Legend is removed from the main interface window.

## Changing connection utilization

You can change the utilization percentages.

To change the utilization percentages, complete the following steps.

1. Click the **change** link in the utilization legend.



**FIGURE 123** Utilization Legend in edit mode

2. Enter or select the end percentage you want for the blue line.

When you make a change to the end percentage of a utilization line, you also change the start percentage for the utilization line immediately above the one you changed when you click **apply**. For example, if you change the blue line end percentage to 60 the yellow line start percentage changes to 60 when you click **apply**.

3. Enter or select the end percentage you want for the yellow line.
4. Click the **apply** link.

The new values appear in the utilization legend.

## 11 Changing connection utilization

# Reports

---

## In this chapter

|                                        |     |
|----------------------------------------|-----|
| • Report types .....                   | 319 |
| • Generating reports .....             | 320 |
| • Viewing reports .....                | 320 |
| • Exporting reports .....              | 321 |
| • Printing reports .....               | 322 |
| • Deleting reports .....               | 322 |
| • Generating performance reports ..... | 323 |
| • Generating zoning reports .....      | 324 |

## Report types

Presenting and archiving data about a SAN is equally as important as gathering the data. Through the Management application, you can generate reports about the SAN. You can send the reports to network administrators, support consultants, and others interested in the SAN's architecture, or archive them for future reference.

The following standard report types are available from the **Generate Reports** dialog box:

- **Fabric Ports.** Lists discovered ports including used and unused ports. Port data for each fabric is divided into three parts: Fabric-wide port details, Switch-wide port details, and individual port details.
- **Fabric Summary.** Lists information about discovered fabrics including fabric and switch details, device information, and ISL and trunk summary.

The following device specific reports are available through the **Monitor (Monitor > Performance > Historical Report)** or **Reports** menu and right-click menus:

- **Performance.** Lists historical performance-related data.
- **Zone.** Lists zoning objects.

# Generating reports

To generate reports, complete the following steps.

1. Select **Reports > Generate**.  
The **Generate Reports** dialog box displays.
2. Select the types of reports you want to generate.
  - Fabric Ports
  - Fabric Summary
3. Select the fabrics for which you want to generate reports.
4. Click **OK**.

The generated reports display in the **View Reports** dialog box.

---

**NOTE**  
Hyperlinks in reports are active only as long as the source data is available.





---






5. Click **Close** to close the **View Reports** dialog box.
6. Click **Yes** on the “are you sure you want to close” message.

# Viewing reports

You can view any report generated in the SAN. To view reports, complete the following steps.

1. Select **Reports > View** or click the **View Report** icon.  
The **View Reports** dialog box displays.
2. Select the report you want to view in the **All Reports** list.  
If you do not see the report you want to view, generate it first by following the instructions in [“Generating reports”](#) on page 320.  
You can select reports by Time, Report Type, or User.
3. Use the buttons in the table below to navigate through and resize the report.

| Icon                                                                                | Description                                                                                                           |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  | First—Click to return to the first page in the report. Greyed out when you are on the first page.                     |
|  | Previous—Click to return to the previous page in the report. Grayed out when you are on the first page of the report. |
|  | Next—Click to move to the next page in the report. Grayed out when you are on the last page of the report.            |
|  | Last—Click to move to the last page in the report. Greyed out when you are on the last page of the report.            |

| Icon                                                                              | Description                                                             |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------|
|  | Actual Size—Click to display the report at its actual size.             |
|  | Fit to Page—Click to resize the report to display entirely in the view. |
|  | Fit to Width—Click to resize the report to fit in the view by width.    |
|  | Zoom In—Click to zoom in on the report.                                 |
|  | Zoom Out—Click to zoom out on the report.                               |

4. Click **Show in Browser** to view the selected report in your default browser window.
5. Click **Close** to close the **View Reports** dialog box.
6. Click **Yes** on the “are you sure you want to close” message.

## Exporting reports

To export reports, complete the following steps.

1. Select **Reports > View** or click the **View Report** icon.  
The **View Reports** dialog box displays.
2. Select the report you want to export in the **All Reports** list.  
If you do not see the report you want to export, generate it first by following the instructions in [“Generating reports”](#) on page 320.  
You can select reports by Time, Report Type, or User.
3. Select the format (**PDF**, **HTML**, or **XML**) you want to export to from the list to the left of the **Export** button.
4. Click **Export**.  
The **Save** dialog box displays.
5. Browse to the file location where you want to save the report and click **Save**.
6. Click **Close** to close the **View Reports** dialog box.
7. Click **Yes** on the “are you sure you want to close” message.

## Printing reports

You can print reports through an internet browser.

1. Select **Reports > View**.

The **View Reports** dialog box displays.

2. Select the report you want to print in the left pane of the dialog box.

If you do not see the report you want to view, generate it first by following the instructions in [“Generating reports”](#) on page 320.

---

**NOTE**

Hyperlinks in reports are active only as long as the source data is available.

---

3. Click **Show in Browser**.

The selected report displays in your default Web browser.

4. Select **File > Print** (in the Web browser).

The **Print** dialog box displays.

5. Select the printer to which you want to print and click **Print**.

6. Close the Web browser.

7. Click **Close** in the **View Reports** dialog box.

8. Click **Yes** on the “are you sure you want to close” message.

## Deleting reports

To delete reports, complete the following steps.

1. Select **Reports > View** or click the **View Report** icon.

The **View Reports** dialog box displays.

2. Select the report you want to delete in the **All Reports** list.

If you do not see the report you want to view, generate it first by following the instructions in [“Generating reports”](#) on page 320.

You can select reports by Time, Report Type, or User.

3. Click **Delete Report**.

---

**ATTENTION**

Once you click **Delete Report**, the report is deleted without confirmation.

---

4. Click **Close** to close the **View Reports** dialog box.

5. Click **Yes** on the “are you sure you want to close” message.

## Generating performance reports

To generate a historical performance report for a device, complete the following steps.

1. Select the device for which you want to generate a performance report.
2. Choose one of the following options:
  - Select **Monitor > Performance > Historical Report**.
  - OR
  - Right-click the device and select **Performance > Historical Report**.

The **Historical Performance Table** dialog box displays.
3. Filter the historical data by completing the following steps.
  - a. Select the number of results to display from the **Display** list.
  - b. Select the ports from which you want to gather performance data from the **From** list.
 

If you select **Custom**, complete the following steps.

    1. Select the type of ports from the **Show** list.
    2. Right-click a device in the **Available** table and select **Expand All**.
    3. Select the ports (**Ctrl** or **Shift** + click to select multiple ports.) from which you want to gather performance data from the **Available** table and click the right arrow button. The selected ports move to the Select Ports table.
    4. Click **OK**.
  - c. Select the historical period from which you want to gather performance data from the **For** list.
 

If you select **Custom**, complete the following steps.

    1. Select the **Last** option and enter the number of minutes, hours, or days.
    - OR
    - Select the **From** option and enter the date and time.
    2. Click **OK**.
  - d. Select the granularity at which you want to gather performance data from the **Granularity** list.
  - e. Select the measure by which you want to gather performance data from the **Measures** list.
 

To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.
  - f. Save this configuration by selecting **Save**.
 

The **Save Favorites** dialog box displays. This enables you to save the selected configuration so that you can use it to generate the same type of report at a later date.

    1. Enter a name for the configuration in the **Favorites Name** field.
    2. Click **OK**.

- g. Click **Apply**.

The selected report automatically displays in the **View Reports** dialog box.

---

**NOTE**

Hyperlinks in reports are active only as long as the source data is available.

---

To print the selected report, refer to [“Printing reports”](#) on page 322.

To export the selected report, refer to [“Exporting reports”](#) on page 321.

To delete the selected report, refer to [“Deleting reports”](#) on page 322.

4. Click the close button (X) to close the **View Reports** dialog box.
  5. Click the close button (X) to close the **Historical Performance Table** dialog box.
- For more information about performance, refer to [“Performance Data”](#) on page 287.

## Generating zoning reports

The Management application enables you to generate a report for the current zone DB in the fabric. To generate a report for the edited zone DB, you must save it to the fabric first. Make sure no one else is making changes to the same area prior to submitting or your changes may be lost.

To generate zoning reports, complete the following steps.

1. Select **Configure > Zoning** or right-click the device and select **Zoning**.  
The **Zoning** dialog box displays.
2. Click **Report**.
3. Click **OK** on the message.

The selected report automatically displays in the **View Reports** dialog box.

---

**NOTE**

Hyperlinks in reports are active only as long as the source data is available.

---

To print the selected report, refer to [“Printing reports”](#) on page 322.

To export the selected report, refer to [“Exporting reports”](#) on page 321.

To delete the selected report, refer to [“Deleting reports”](#) on page 322.

4. Click **Close** to close the **View Reports** dialog box.
5. Click **Yes** on the “are you sure you want to close” message.

For more information about zoning, refer to [“Zoning”](#) on page 603.

# Port Fencing

---

## In this chapter

- [About port fencing](#) ..... 325
- [Thresholds](#) ..... 326
- [Adding thresholds](#) ..... 329
- [Removing thresholds](#) ..... 349

## About port fencing

Port Fencing allows you to protect your SAN from repeated operational or security problems experienced by ports. Use Port Fencing to set threshold limits for the number of specific port events permitted during a given time period on the selected object.

Port Fencing objects include the SAN, Fabrics, Directors, Switches (physical), Virtual Switches, Ports, as well as Port Types (E\_port, F\_port, and FX\_port). Use Port Fencing to directly assign a threshold to these objects. When a switch does not support Port Fencing, a “No Fencing Changes” message displays in the **Threshold** field in the **Ports** table.

If the port detects more events during the specified time period, the device firmware blocks the port, disabling transmit and receive traffic until you investigate, solve the problem, and manually unblock the port.

Physical fabrics, directors, switches, port types, and ports display when you have the privileges to manage that object and are indicated by the standard product icons.

---

### NOTE

Port Fencing displays any existing thresholds discovered on manageable fabrics, directors, and switches running firmware versions M-EOS 9.X or Fabric OS 6.2 or later.

---

## Port Fencing requirements

To configure port fencing, the following requirements must be met:

- All Fabric OS devices must have Fabric Watch and must be running firmware Fabric OS 6.2 or later.
- All M-EOS devices must be running firmware M-EOS 9.X or later.
- All M-EOS devices must be discovered directly using MPI.

## Thresholds

You can create thresholds, which you can then assign to available objects in the tree. Port Fencing threshold types include the following:

- C3 Discard Frames (Fabric OS only)
- Invalid CRCs (Fabric OS only)
- Invalid Words (Fabric OS only)
- Link (M-EOS only)
- Link Reset (Fabric OS only)
- Protocol Errors (M-EOS and Fabric OS)
- Security (M-EOS)
- State Change (Fabric OS only)

---

### NOTE

You can create up to 16 thresholds for M-EOS devices.

---



---

### NOTE

Fabric OS devices are allowed only 2 defined thresholds (one default and one custom) for each threshold type and only one of these thresholds can be active on the device.

---

During the dynamic operation of a Fabric, any port could be any type. For example, a technician could disconnect a port from a switch and reconnect that port to a storage port, or the port could change from an E\_port to an F\_port. Therefore, when calculating the **Affected Ports** value the Management application does not look for the current port type, but looks at the policy priority level in relation to the other policies currently assigned to this switch.

When there are two or more policies on a switch, the total number of **Affected Ports** may be more than the total number of ports on the switch (the same port may adopt different policies depending on changes in the port's port type).

For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

## C3 Discard Frames threshold

---

### NOTE

This threshold is only available for Fabric OS devices running 6.3 or later.

---



---

### NOTE

The C3 Discard Frames threshold cannot be applied to an E port.

---

Use this type of threshold to block a port when a C3 Discard Frames violation meets the Fabric OS switch threshold. This threshold is only supported on the following devices:

- 40-port, 8 Gbps FC Switch
- 80-port, 8 Gbps FC Switch
- 8 Gbps 12-port Embedded Switch
- 8 Gbps 24-port Embedded Switch

- 8 Gbps 16-port Embedded Switch
- 8 Gbps 24-port Embedded Switch
- 24 - 8 Gbps FC Port, 8 - 10 Gbps CEE Port Switch
- 384-port Backbone Chassis
- 192-port Backbone Chassis
- 8 Gbps Encryption Switch
- Encryption Blade
- FC 8 GB 16-port Blade
- FC 8 GB 32-port Blade
- FC 8 GB 48-port Blade

## Invalid CRCs threshold

---

**NOTE**

This threshold is only available for Fabric OS devices.

---

Use this type of threshold to block a port when an Invalid CRCs violation meets the Fabric OS switch threshold.

## Invalid words threshold

---

**NOTE**

This threshold is only available for Fabric OS devices.

---

Use this type of threshold to block a port when an Invalid Words violation meets the Fabric OS switch threshold.

## Link threshold

---

**NOTE**

This threshold is only available for M-EOS devices.

---

Use this type of threshold to block a port when a Link Level (Hot I/O) error meets the threshold. A Link Level (Hot I/O) occurs when an active loop port repeatedly receives a loop initialization primitive sequence error or an active non-loop port repeatedly receives a line repeater, offline sequence, or not operational sequence error.

## Link Reset threshold

---

**NOTE**

This threshold is only available for Fabric OS devices.

---

Use this type of threshold to block a port when the link timeout errors meet the threshold.

## Protocol error threshold

Use Protocol Error thresholds to block a port when one of the following protocol errors meet the threshold:

- ISL Bouncing–ISL has repeatedly become unavailable due to link down events.
- ISL Segmentation (M-EOS only)–ISL has repeatedly become segmented.
- ISL Protocol Mismatch–ISL has been repeatedly put into the Invalid Attachment state due to a protocol error.

## State Change threshold

---

**NOTE**

This threshold is only available for Fabric OS devices running 6.3 or later.

---

Use this type of threshold to block a port when a state change violation type meets the Fabric OS switch threshold.

For 4 Gbps Router, Extension Switches and Blades only, when you apply this threshold on an E Port, the threshold is also applied to the VE Ports (internally by Fabric OS).

## Security threshold

---

**NOTE**

This threshold is only available for M-EOS devices.

---

Use this type of threshold to block a port when one of the following security violations occur:

- Authentication–the switch has repeatedly become unavailable due to authentication events.
- Fabric Binding–the switch has repeatedly become unavailable due to fabric binding events.
- Switch Binding–the switch has repeatedly become unavailable due to switch binding events. Switch Binding is enabled through a product's Element Manager.
- Port Binding–the switch has repeatedly become unavailable due to port binding events.
- ISL Security–(Generic Security Error) the switch on the other side of the ISL has detected a specific security violation, but is only able to indicate that a generic security violation has occurred or a security configuration mismatch was detected.
- N\_port Connection Not Allowed–the switch has repeatedly become unavailable due to N\_port connection not allowed events.

# Adding thresholds

The Management application allows you to create Invalid CRCs, Invalid words, Link, Link Reset, Protocol Error, Security, and Sync Loss thresholds.

## Adding a C3 Discard Frames threshold

**NOTE**  
This threshold is only available for Fabric OS devices running 6.3 or later.

To add an C3 Discard Frames threshold, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays (Figure 124).

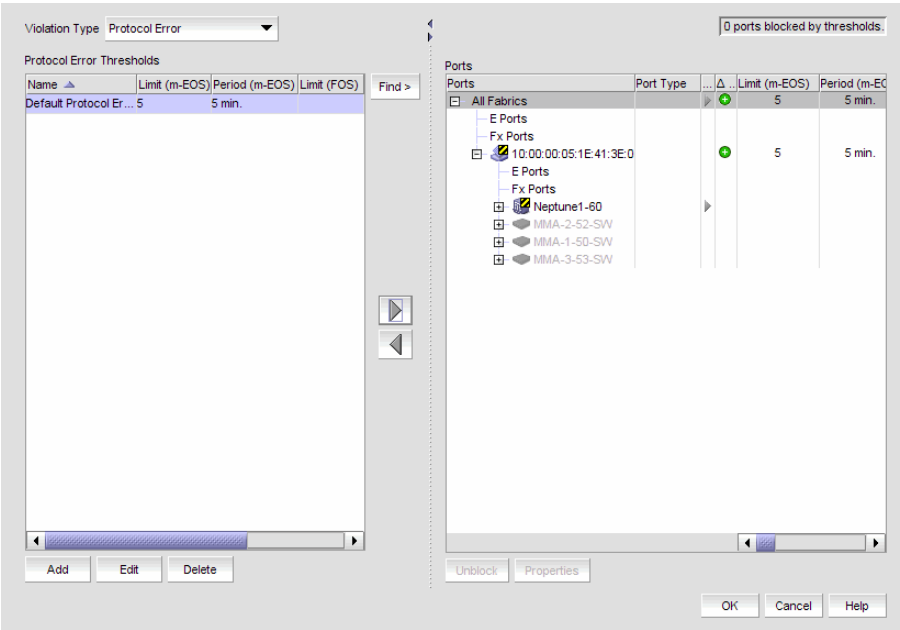


FIGURE 124 Port Fencing dialog box

2. Select **C3 Discard Frames (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

The **Add C3 Discard Frames Threshold** dialog box displays.

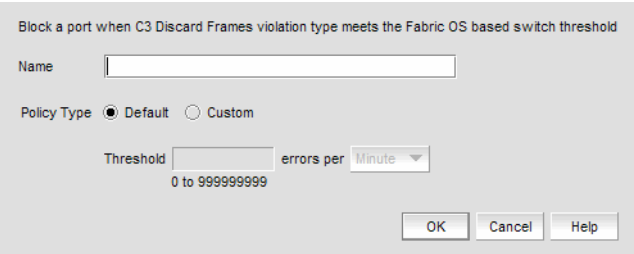


FIGURE 125 Add C3 Discard Frames Threshold dialog box

## 13 Adding thresholds

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
  - **Default**—Uses device defaults. Go to [step 8](#).
  - **Custom**—Uses your selections. Continue with [step 6](#).
6. Enter the number of C3 discarded frames allowed for the threshold in the **Threshold errors** field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
  - **None**—the port is blocked as soon as the specified number of C3 discarded frames allowed is met.
  - **Second**—the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a second.
  - **Minute**—the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a minute.
  - **Hour**—the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a hour.
  - **Day**—the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a day.
8. Click **OK** to add the C3 discarded frames threshold to the table and close the **Add C3 Discard Frames Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.
9. Click **OK** on the **Port Fencing** dialog box.

## Adding an Invalid CRCs threshold

### NOTE

This threshold is only available for Fabric OS devices.

To add an Invalid CRCs threshold, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select **Invalid CRCs (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

The **Add Invalid CRCs Threshold** dialog box displays.

**FIGURE 126** Add Invalid CRCs Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
  - **Default**—Uses device defaults. Go to [step 8](#).
  - **Custom**—Uses your selections. Continue with [step 6](#).
6. Enter the number of invalid CRCs allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
  - **None**—the port is blocked as soon as the specified number of invalid CRCs allowed is met.
  - **Second**—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a second.
  - **Minute**—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a minute.
  - **Hour**—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a hour.
  - **Day**—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a day.
8. Click **OK** to add the Invalid CRCs threshold to the table and close the **Add Invalid CRCs Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Adding an Invalid Words threshold

### NOTE

This threshold is only available for Fabric OS devices.

To add an Invalid Words threshold, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select **Invalid Words (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

The **Add Invalid Words Threshold** dialog box displays.

**FIGURE 127** Add Invalid Words Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
  - **Default**—Uses device defaults. Go to [step 8](#).
  - **Custom**—Uses your selections. Continue with [step 6](#).
6. Enter the number of invalid words allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
  - **None**—the port is blocked as soon as the specified number of invalid words allowed is met.
  - **Second**—the port is blocked as soon as the specified number of invalid words allowed is reached within a second.
  - **Minute**—the port is blocked as soon as the specified number of invalid words allowed is reached within a minute.
  - **Hour**—the port is blocked as soon as the specified number of invalid words allowed is reached within a hour.
  - **Day**—the port is blocked as soon as the specified number of invalid words allowed is reached within a day.
8. Click **OK** to add the Invalid Words threshold to the table and close the **Add Invalid Words Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Adding a Link threshold

---

**NOTE**

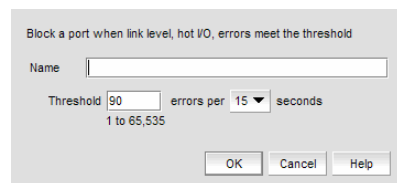
This threshold is only available for M-EOS devices.

---

To add Link thresholds, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select **Link** from the **Violation Type** list.
3. Click **Add**.

The **Add Link Threshold** dialog box displays ([Figure 128](#)).

The image shows a dialog box titled "Block a port when link level, hot I/O, errors meet the threshold". It contains a "Name" text field, a "Threshold" field with the value "90" and a range "1 to 65,535" below it, and a dropdown menu for "errors per" with the value "15" and the unit "seconds" to its right. At the bottom are three buttons: "OK", "Cancel", and "Help".

**FIGURE 128** Add Link Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select the number of link errors allowed for the threshold from the **Threshold** errors list.
6. Select the time period for the threshold (in minutes) from the **errors per** list.
7. Click **OK** to add the Link threshold to the table and close the **Add Link Threshold** dialog box.  
To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.
8. Click **OK** on the **Port Fencing** dialog box.

## Adding a Link Reset threshold

### NOTE

This threshold is only available for Fabric OS devices.

Use this threshold to block a port when a Link Reset violation meets the Fabric OS switch threshold.

To add a Link Reset threshold, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select **Link Reset (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

The **Add Link Reset Threshold** dialog box displays.

**FIGURE 129** Add Link Reset Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
  - **Default**—Uses device defaults. Go to [step 8](#).
  - **Custom**—Uses your selections. Continue with [step 6](#).
6. Enter the number of link resets allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
  - **None**—the port is blocked as soon as the specified number of link resets allowed is met.
  - **Second**—the port is blocked as soon as the specified number of link resets allowed is reached within a second.
  - **Minute**—the port is blocked as soon as the specified number of link resets allowed is reached within a minute.
  - **Hour**—the port is blocked as soon as the specified number of link resets allowed is reached within a hour.
  - **Day**—the port is blocked as soon as the specified number of link resets allowed is reached within a day.

8. Click **OK** to add the Link Resets threshold to the table and close the **Add Link Reset Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Adding a Protocol Error threshold

To add a Protocol Error threshold, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select **Protocol Error** from the **Violation Type** list.
3. Click **Add**.

The **Add Protocol Error Threshold** dialog box displays.

Block a port when one of the following ISL protocol error types meets the threshold:

- ISL Bouncing
- ISL Segmentation (m-EOS only)
- ISL Protocol Mismatch

Name

☐ m-EOS

Threshold  errors per  minutes

☐ FOS

Policy Type ☐ Default ☐ Custom

Threshold  errors per

0 to 999999999

**FIGURE 130** Add Protocol Error Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. (M-EOS devices only) Select the **M-EOS** check box.
  - a. Select the number of protocol errors allowed for the threshold from the **Threshold** errors list.
  - b. Select the time period for the threshold (in minutes) from the **errors per** list.
6. (Fabric OS devices only) Select the **Fabric OS** check box.
  - a. Select one of the following options:
    - Default—Uses device defaults. Go to [step 7](#).
    - Custom—Uses your selections. Continue with [step b](#).
  - b. Enter the number of protocol errors allowed for the threshold from the **Threshold** errors field.

## 13 Adding a State Change threshold

- c. Select the time period for the threshold from the **errors per** list. The following choices are available:
  - None—the port is blocked as soon as the specified number of protocol errors allowed is met.
  - Second—the port is blocked as soon as the specified number of protocol errors allowed is reached within a second.
  - Minute—the port is blocked as soon as the specified number of protocol errors allowed is reached within a minute.
  - Hour—the port is blocked as soon as the specified number of protocol errors allowed is reached within a hour.
  - Day—the port is blocked as soon as the specified number of protocol errors allowed is reached within a day.
7. Click **OK** to add the protocol errors threshold to the table and close the **Add Protocol Error Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.
8. Click **OK** on the **Port Fencing** dialog box.

## Adding a State Change threshold

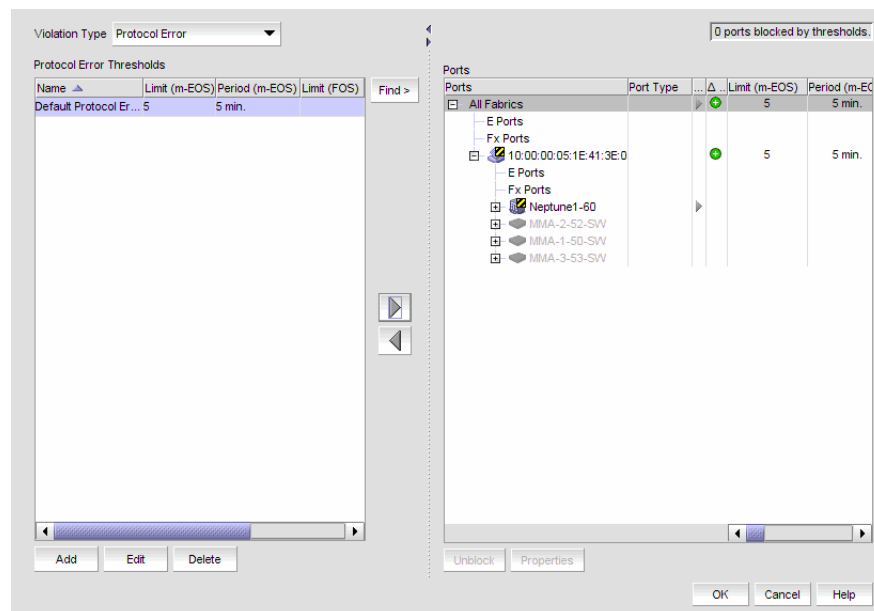
### NOTE

This threshold is only available for Fabric OS devices running 6.3 or later.

To add an State Change threshold, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays ([Figure 124](#)).



**FIGURE 131** Port Fencing dialog box

2. Select **State Change (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

The **Add State Change Threshold** dialog box displays.

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
  - **Default**—Uses device defaults. Go to [step 8](#).
  - **Custom**—Uses your selections. Continue with [step 6](#).
6. Enter the number of state changes allowed for the threshold in the **Threshold errors** field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
  - **None**—the port is blocked as soon as the specified number of state changes allowed is met.
  - **Second**—the port is blocked as soon as the specified number of state changes allowed is reached within a second.
  - **Minute**—the port is blocked as soon as the specified number of state changes allowed is reached within a minute.
  - **Hour**—the port is blocked as soon as the specified number of state changes allowed is reached within a hour.
  - **Day**—the port is blocked as soon as the specified number of state changes allowed is reached within a day.
8. Click **OK** to add the state changes threshold to the table and close the **Add State Change Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Adding a Security threshold

### NOTE

This threshold is only available for M-EOS devices.

To add a Security threshold, complete the following steps.

1. Select **Configure > Port Fencing**.
2. Select **Security** from the **Violation Type** list.
3. Click **Add**.

The **Add Security Threshold** dialog box displays ([Figure 126](#)).

Block a port when one of the following security violation types meets the threshold:

- Authentication
- Fabric Binding
- Switch Binding
- Port Binding
- ISL Security
- N Port Connection Not Allowed

Name

Threshold  violations per  minutes

**FIGURE 132** Add Security Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select the number of port events allowed for the threshold from the **Threshold** errors list.
6. Select the time limit for the threshold from the **violations per** list.
7. Click **OK** to add the security threshold to the table and close the **Add Security Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

8. Click **OK** on the **Port Fencing** dialog box.

## Assigning thresholds

You can assign thresholds to any active object in the **Ports** table. You can only assign one threshold to an object at a time. If you assign a threshold to a switch, director, or fabric object, or to the All Fabrics object, the threshold is assigned to all subordinate objects (which do not have a directly assigned threshold) in the tree.

However, if an object inherits a threshold from another object above it in the hierarchy, you cannot remove that inherited threshold directly from the subordinate object. You must either remove the threshold from the higher object to which it was directly assigned or directly assign a different threshold to the subordinate object.

To assign an existing threshold to fabric, director, switch, port type, and port objects, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select the threshold you want to assign from the **Thresholds** table.
4. Select the objects (All Fabrics, Fabric, Director, Switch, Port Type, and/or Port) to which you want to assign the threshold from the **Ports** table.
5. Click the right arrow.

A directly assigned icon ( ► ) displays next to the objects you selected in the **Ports** table to show that the threshold was applied at this level and was inherited by every subordinate object below it in the tree (if not affected by lower level direct assignments).

An added icon ( + ) appears next to every object in the tree to which the new threshold is applied.

6. Click **OK** on the **Port Fencing** dialog box.

## Unblocking a port

The Management application allows you to unblock a port (only if it was blocked by Port Fencing) once the problem that triggered the threshold is fixed. When a port is blocked an Attention icon ( ⚠ ) displays next to the port node.

To unblock a port, complete the following steps.

1. Select **Configure > Port Fencing**.  
The Port Fencing dialog box displays.
2. Right-click anywhere in the Ports table and select **Expand**.
3. Select a blocked port from the Ports table.
4. Click **Unblock**.
5. Click **OK** on the message.

If you did not solve the root problem, the threshold will trigger again.

6. Click **OK** on the Port Fencing dialog box.

## Avoiding port fencing inheritance

When you directly assign a threshold to an object, the threshold is inherited by all subordinate objects in the tree (unless they already have directly assigned thresholds). You cannot remove an inherited threshold from a subordinate object. However, the Management application allows you to effectively avoid inheritance for individual subordinate objects while maintaining inheritance for other subordinate objects. To avoid inheritance for an individual subordinate object, you must create a new threshold with a maximum limit of events allowed and a minimum time period, then assign the new threshold to the subordinate object.

To turn off port fencing inheritance, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.

3. Click **Add**.

The **Add Type Threshold** dialog box displays.

4. Type a name for the new threshold (for example, AvoidProtocolError) in the **Name** field.
5. Select or enter the maximum number of errors or violations allowed in the **Threshold errors/violations** field.
6. Select the minimum time period available from the **Threshold minutes/seconds** list.
7. Click **OK** on the **Add Type Threshold** dialog box.
8. Click **OK** on the **Port Fencing** dialog box.

## Editing thresholds

The Management application allows you to edit the name, number of events needed, and time period of ISL Protocol, Link, and Security thresholds.

## Editing a C3 Discard Frames threshold

---

### NOTE

This threshold is only available for Fabric OS devices.

---

To edit a C3 Discard Frames threshold, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select **C3 Discard Frames (Fabric OS only)** from the **Violation Type** list.

3. Select the threshold you want to change and click **Edit**.

The **Edit C3 Discard Frames** dialog box displays.

**FIGURE 133** Edit C3 Discard Frames Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
  - **Default**—Uses device defaults. Go to [step 8](#).
  - **Custom**—Uses your selections. Continue with [step 6](#).
6. Change the number of discarded frames allowed for the threshold in the **Threshold** field, if necessary.
7. Change the time period for the threshold from the **errors per** list, if necessary.
8. Click **OK** on the **Edit C3 Discard Frames Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Editing an Invalid CRCs threshold

### NOTE

This threshold is only available for Fabric OS devices.

To edit an Invalid CRCs threshold, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select **Invalid CRCs (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

The **Edit Invalid CRCs Threshold** dialog box displays.

**FIGURE 134** Edit Invalid CRCs Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
  - Default—Uses device defaults. Go to [step 8](#).
  - Custom—Uses your selections. Continue with [step 6](#).
6. Change the number of port events allowed for the threshold in the **Threshold** field, if necessary.
7. Change the time period for the threshold from the **errors per** list, if necessary.
8. Click **OK** on the **Edit Invalid CRCs Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to “[Assigning thresholds](#)” on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Editing an Invalid Words threshold

### NOTE

This threshold is only available for Fabric OS devices.

To edit an Invalid Words threshold, complete the following steps.

1. Select **Configure > Port Fencing**.
- The **Port Fencing** dialog box displays.
2. Select **Invalid Words (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

The **Edit Invalid Words Threshold** dialog box displays.

**FIGURE 135** Edit Invalid Words Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
  - Default—Uses device defaults. Go to [step 8](#).
  - Custom—Uses your selections. Continue with [step 6](#).
6. Change the number of port events allowed for the threshold in the **Threshold** field, if necessary.
7. Change the time period for the threshold from the **errors per** list, if necessary.

8. Click **OK** on the **Edit Invalid Words Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Editing a Link threshold

### NOTE

This threshold is only available for M-EOS devices.

To edit a Link threshold, complete the following steps.

1. Select **Configure > Port Fencing**.
- The **Port Fencing** dialog box displays.
2. Select **Link** from the **Violation Type** list.
3. Click **Edit**.

The **Edit Link Threshold** dialog box displays.

**FIGURE 136** Edit Link Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Change the number of link events allowed for the threshold from the **Threshold** errors list.
6. Select the time period for the threshold (in minutes) from the **errors per** list.
7. Click **OK** on the **Edit Link Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

8. Click **OK** on the **Port Fencing** dialog box.

## Editing a Link Reset threshold

### NOTE

This threshold is only available for Fabric OS devices.

To edit a Link Reset threshold, complete the following steps.

1. Select **Configure > Port Fencing**.
2. Select **Link Reset (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

The **Edit Link Reset Threshold** dialog box displays.

**FIGURE 137** Edit Link Reset Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
  - **Default**—Uses device defaults. Go to [step 8](#).
  - **Custom**—Uses your selections. Continue with [step 6](#).
6. Change the number of port events allowed for the threshold in the **Threshold** field, if necessary.
7. Change the time period for the threshold from the **errors per** list, if necessary.
8. Click **OK** on the **Edit Link Reset Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Editing a Protocol Error threshold

To edit a Protocol Error threshold, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select **Protocol Error** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

The **Edit Protocol Error Threshold** dialog box displays.

**FIGURE 138** Edit Protocol Error Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. (M-EOS devices only) Change the **M-EOS** Protocol Error thresholds by completing the following steps.
  - a. Change the number of protocol errors allowed for the threshold from the **Threshold** errors list, if necessary.
  - b. Change the time period for the threshold (in minutes) from the **errors per** list, if necessary.
6. (Fabric OS devices only) Change the **Fabric OS** Protocol Error thresholds by completing the following steps.
  - a. Select one of the following options:
    - Default—Uses device defaults. Go to [step 7](#).
    - Custom—Uses your selections. Continue with [step b](#).
  - b. Change the number of protocol errors allowed for the threshold from the **Threshold** errors list, if necessary.
  - c. Change the time period for the threshold from the **errors per** list, if necessary.
7. Click **OK** on the **Edit Protocol Error Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

8. Click **OK** on the **Port Fencing** dialog box.

## Editing a State Change threshold

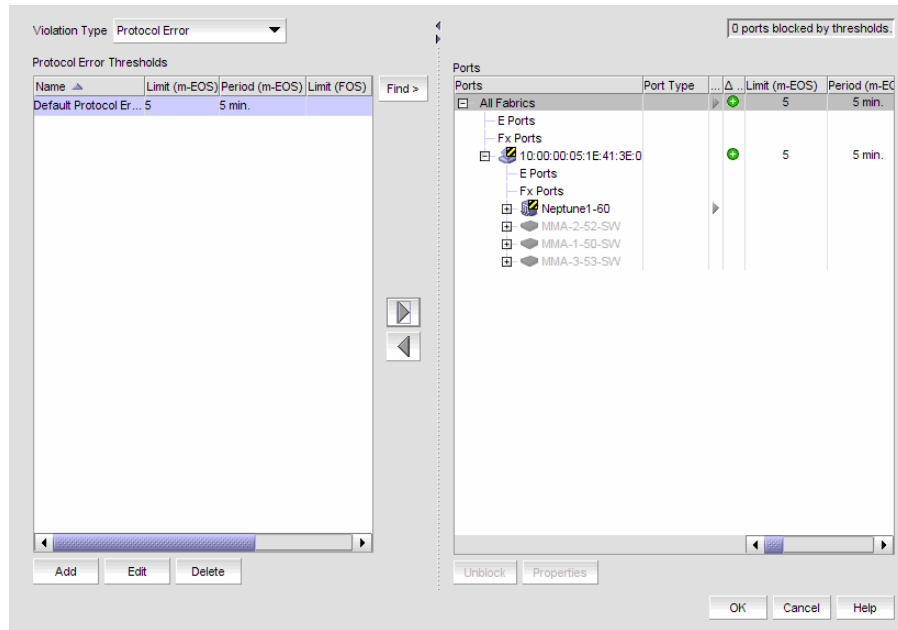
### NOTE

This threshold is only available for Fabric OS devices running 6.3 or later.

To edit an State Change threshold, complete the following steps.

1. Select **Configure > Port Fencing**.

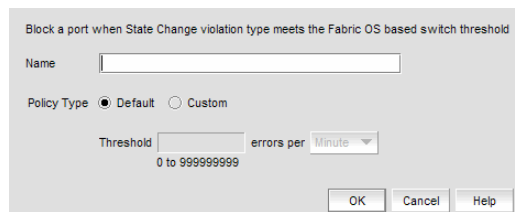
The **Port Fencing** dialog box displays (Figure 124).



**FIGURE 139** Port Fencing dialog box

2. Select **State Change (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

The **Edit State Change Threshold** dialog box displays.



**FIGURE 140** Edit State Change Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
  - Default—Uses device defaults. Go to [step 8](#).
  - Custom—Uses your selections. Continue with [step 6](#).

6. Edit the number of state changes allowed for the threshold in the **Threshold** errors field, if necessary.
7. Change the time period for the threshold from the **errors per** list, if necessary. The following choices are available:
  - None—the port is blocked as soon as the specified number of invalid CRCs allowed is met.
  - Second—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a second.
  - Minute—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a minute.
  - Hour—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a hour.
  - Day—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a day.
8. Click **OK** to add the state change threshold to the table and close the **Edit State Change Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

9. Click **OK** on the **Port Fencing** dialog box.

## Editing a Security threshold

### NOTE

This threshold is only available for M-EOS devices.

To edit a Security threshold, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select **Security** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

The **Edit Security Threshold** dialog box displays.

Block a port when one of the following security violation types meets the threshold:

- Authentication
- Fabric Binding
- Switch Binding
- Port Binding
- ISL Security
- N Port Connection Not Allowed

Name

Threshold  violations per  minutes

**FIGURE 141** Edit Security Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.

5. Change the number of port events allowed for the threshold from the **Threshold** errors list, if necessary.
6. Change the time period for the threshold from the **violations per** list, if necessary.
7. Click **OK** on the **Edit Security Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning thresholds”](#) on page 339.

8. Click **OK** on the **Port Fencing** dialog box.

### Finding assigned thresholds

The Management application allows you to find all ports with a specific threshold applied.

---

#### NOTE

This search is performed on the threshold name. Since Fabric OS devices do not retain the threshold name, the ability to search for a threshold on a Fabric OS device is not available in most cases.

---

To find assigned thresholds, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select a threshold type from the **Violation Type** list.
3. Select a threshold from the **Threshold** table.
4. Click **Find**.
5. Every port which uses the selected threshold is highlighted in the **Ports** table.
6. Click **OK** on the **Port Fencing** dialog box.

### Viewing thresholds

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select a threshold type from the **Violation Type** list.
3. Review the **Thresholds** and **Ports** tables.
4. Repeat [step 2](#) and [step 3](#), as necessary.
5. Click **OK** on the **Port Fencing** dialog box.

## Viewing all thresholds on a specific device

To view all thresholds assigned to a specific switch, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Right-click anywhere in the **Ports** table and select **Expand**.
3. Right-click the device for which you want to view threshold information and select **Switch Thresholds**.

The **Switch Thresholds** dialog box displays with a list of all thresholds assigned to the selected switch.

4. Review the **Thresholds** table.
5. Click **Close** on the **Switch Thresholds** dialog box.
6. Click **OK** on the **Port Fencing** dialog box.

## Removing thresholds

When you assign a new threshold to an object, the threshold that was active on that object is automatically removed. The Management application also allows you to remove thresholds from an individual Fabric, Switch, or Switch Port, from all Fabrics, Switches, and Switch Ports at once, as well as from the **Threshold** table.

### Removing thresholds from individual objects

To remove thresholds from the All Fabrics object, an individual Fabric, Chassis group, Switch, or Switch Port, complete the following steps.

1. Select **Configure > Port Fencing**.
- The **Port Fencing** dialog box displays.
2. Select a threshold type from the **Violation Type** list.
  3. Select the object with the threshold you want to remove in the **Ports** table.
  4. Click the left arrow.

---

#### NOTE

If the selected object inherits a threshold assignment from an object higher in the tree, you cannot remove the threshold. However, you may assign a different threshold directly to the selected subordinate objects or change the assignment on the higher object.

---

A removed icon (–) displays next to every instance where the threshold was removed from a selected object and it does not inherit a threshold from higher in the tree.

If an inherited threshold replaces the removed threshold, an added icon (+) displays next to every instance where the threshold was replaced.

## 13 Removing thresholds from the thresholds table

A directly assigned icon ( ► ) displays next to each object with an assigned threshold which does not inherit a threshold from higher in the tree.

---

### NOTE

If you remove a threshold from All Fabrics, it removes the threshold from individual Fabrics, switches, and switch ports in all Fabrics except for a Chassis group. You must remove repeat the procedure for the Chassis group.

---

5. Click **OK** on the **Port Fencing** dialog box.


## Removing thresholds from the thresholds table

To remove thresholds from all Fabrics, Switches, and Switch Ports as well as the **Threshold** table, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select the threshold you want to remove in the **Thresholds** table.
4. Click **Delete**.

A removed icon (  ) displays next to the selected threshold in the **Thresholds** table when you click **Delete**.

5. Click **OK** on the **Port Fencing** dialog box.

# Role-Based Access Control

## In this chapter

- [Users](#) ..... 351
- [Roles](#)..... 355
- [Resource groups](#) ..... 358

## Users

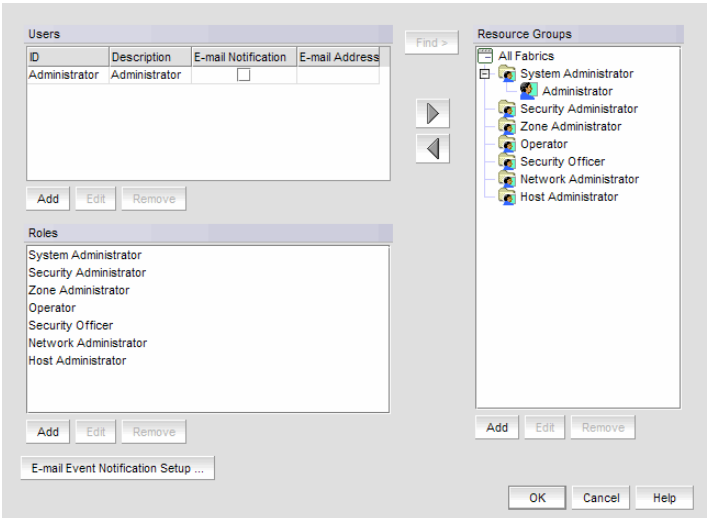
The Management application enables you to create users, roles, and resource groups.

When you set up users, you can add, change, or remove users as well as configure event notification.

### Viewing the list of users

Select **Server > Users**.

The **Server Users** dialog box displays users, their event notification settings, and their e-mail addresses ([Figure 142](#)). The Management application is delivered with a default user 'Administrator' which has a default password. The defaults are Administrator and password, respectively. The Management application provides seven pre-configured roles (System Administrator, Security Administrator, Zone Administrator, Operator, Security Officer, Network Administrator, and Host Administrator). For more information about default roles and access levels, refer to [“About Roles and Access Levels”](#) on page 717.



**FIGURE 142** Server Users dialog box

## Adding a user account

### NOTE

You must have the User Management privilege to perform this task.

To add a user, complete the following steps.

1. Select **Server > Users**.

The **Server Users** dialog box displays.

2. Click **Add**.

The **New User** dialog box displays (Figure 143).

The screenshot shows a 'New User' dialog box with the following fields and controls:

- Description**: A text input field.
- User ID**: A text input field.
- Password**: A text input field.
- Retype Password**: A text input field.
- E-mail Notification**: A section containing an ☐ **Enable** checkbox and a [Filter](#) link.
- E-mail Address**: A large text area for multiple addresses.
- Buttons**: **OK**, **Cancel**, and **Help** buttons at the bottom right.

**FIGURE 143** New User dialog box

3. Type the description of the user in the **Description** field.
4. Type a unique user name (127-character limit) for the user in the **User ID** field.
5. Type the user's password (127-character limit) in the **Secure Password** and **Retype Password** fields.
6. Select the **Enable** option to enable e-mail notification for the user.

### NOTE

You must have E-mail Event Notification Setup privileges to enable e-mail notification.

A message may display stating that you have enabled event notification for this user but event notification for the SAN is turned off, do you want to enable event notification for the SAN. Click **Yes**.

7. Type the user's e-mail addresses in the **E-mail Address** field, separating multiple addresses with a semicolon (;).
8. Click the **Filter** link to specify the event types for which to send e-mail notification to this user.  
For detailed instructions, refer to "[Filtering event notifications for a user](#)" on page 353.
9. Click **OK** to save your changes and close the **Add User** dialog box.
10. Click **OK** on the message.

The new user displays on the **Server Users** dialog box.

11. Click **OK** to close the **Server Users** dialog box.

## Editing a user account

---

**NOTE**

You must have the User Management privilege to perform this task.

---

To edit a user, complete the following steps.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Select the user whose information you want to edit in the **Users** table.
3. Click **Edit**.  
The **Edit User** dialog box displays.
4. Edit the information as necessary.
5. Click **OK** to save your changes and close the **Edit User** dialog box.
6. Click **OK** on the message.  
The edited information displays on the **Server Users** dialog box.
7. Click **OK** to close the **Server Users** dialog box.

## Filtering event notifications for a user

The application provides notification of many different types of SAN events. If a user only wants to receive notification of certain events, you can filter the events specifically for that user.

---

**NOTE**

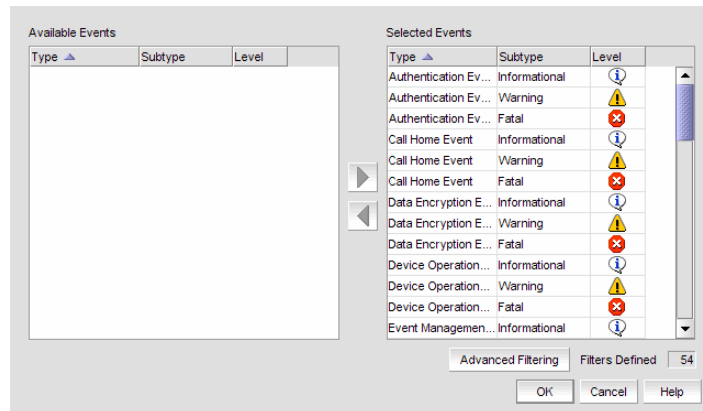
The e-mail filter in the Management application is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box.

---

To configure event notifications for a user, complete the following steps.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Select a user and click **Edit** in the **Users** table.  
The **Edit User** dialog box displays.
3. Select the **E-Mail Notification Enable** check box and click the **Filter** link.  
The **Define Filter** dialog box displays ([Figure 144](#)). The **Selected Events** table includes the events of which this user is notified. The **Available Events** table includes all other events.

## 14 Removing a user account



**FIGURE 144** Define Filter dialog box

4. Move events between the tables by selecting the event and clicking the appropriate arrow.
5. Set up advanced event filtering by clicking **Advanced Filtering**.  
For more information about advanced event filtering, refer to [“Setting up advanced event filtering for a user”](#) on page 275.
6. Click **OK**.  
The **Server Users** dialog box displays.
7. Turn on event notification for the user by selecting the check box in the **E-mail Notification** column of the **Users** table.
8. Click **OK** to save your changes and close the **Server Users** dialog box.

## Removing a user account

### NOTE

You must have the User Management privilege to perform this task.

### ATTENTION

You are prompted for confirmation before the user's account is removed. However, if users are logged in when you remove their accounts, they receive a message that states that their client has been disconnected. They are immediately logged out after they click **OK** on the message.

When you remove a user, the user is automatically removed from any resource groups to which it is assigned.

To remove a user, complete the following steps.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Select the user account you want to remove.
3. Click **Remove**.

4. Click **OK** on the confirmation message.  
The selected user is removed from the **Server Users** dialog box.
5. Click **OK** to close the **Server Users** dialog box.

## Roles

The Management application enables you to set privileges for individual users, which enhances the security of your SAN.

### Creating a user role

#### NOTE

You must have the User Management privilege to perform this task.

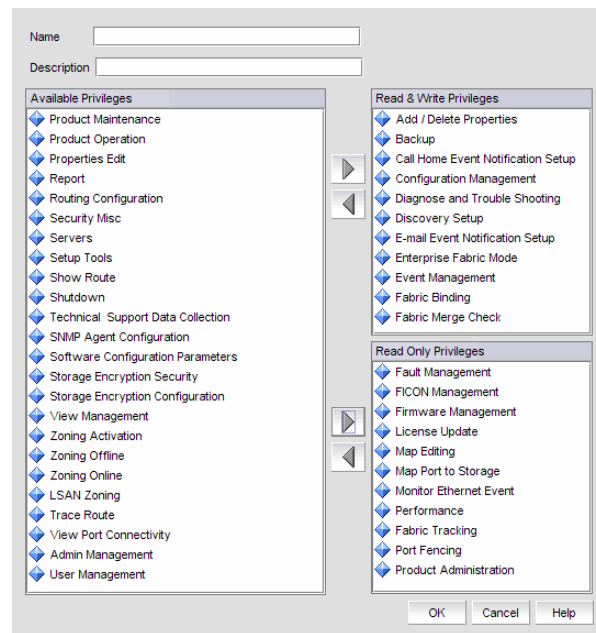
#### NOTE

You must add at least one user privilege to either the **Read & Write Privileges** list or the **Read Only Privileges** list before you can save the user role.

When you create a user role it is automatically assigned to all resource groups.

To create a role, complete the following steps.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Click **Add** under the **Roles** table.  
The **User Roles Properties** dialog box displays (Figure 145).



**FIGURE 145** User Role Properties dialog box

3. Enter a name for the role in the **Name** field.
4. (Optional) Enter a description for the role in the **Description** field.
5. Add Read and Write access by completing the following steps.
  - a. In the **Available Privileges** list, select features to which you want to allow read and write access. Press **CTRL** and click to select multiple features.
  - b. Click the right arrow next to the **Read & Write Privileges** list.  
The features are moved to the **Read & Write Privileges** list.
6. Add Read Only access by completing the following steps.
  - a. In the **Available Privileges** list, select features to which you want to allow read only access. Press **CTRL** and click to select multiple features.
  - b. Click the right arrow next to the **Read Only Privileges** list.  
The features are moved to the **Read Only Privileges** list.
7. Click **OK** to save the new role and close the **User Roles Properties** dialog box.  
The new role displays in the **Roles** list of the **Server Users** dialog box. To add users to this role, follow the instructions in [“Assigning a user to a resource group”](#) on page 361.
8. Click **OK** to close the **Server Users** dialog box.

## Editing a user role

---

### NOTE

You must have the User Management privilege to perform this task.

---



---

### NOTE

When a user assigned to the role you are editing is logged in while you are making changes, the Management application forces the user to log out when you save your work.

---

To edit a role, complete the following steps.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Select the role you want to edit in the **Roles** table and click **Edit**.  
The **User Roles Properties** dialog box displays.
3. Edit the name and description for the role in the fields provided, if necessary.
4. Add Read and Write access by completing the following steps.
  - a. In the **Available Privileges** list, select features to which you want to allow read and write access. Press **CTRL** and click to select multiple features.
  - b. Click the right arrow next to the **Read & Write Privileges** list.  
The features are moved to the **Read & Write Privileges** list.

5. Remove Read and Write access by completing the following steps.
  - a. In the **Read & Write Privileges** list, on the left, select features to which you want to remove read and write access. Press **CTRL** and click to select multiple features.
  - b. Click the left arrow next to the **Available Privileges** list.  
The features are moved to the **Available Privileges** list.
6. Add Read Only access by completing the following steps.
  - a. In the **Available Privileges** list, select features to which you want to allow read only access. Press **CTRL** and click to select multiple features.
  - b. Click the right arrow next to the **Read Only Privileges** list.  
The features are moved to the **Read Only Privileges** list.
7. Remove Read Only access by completing the following steps.
  - a. In the **Read Only Privileges** list, on the left, select features to which you want to remove read only access. Press **CTRL** and click to select multiple features.
  - b. Click the left arrow next to the **Available Privileges** list.  
The features are moved to the **Available Privileges** list.
8. Click **OK** to save the role and close the **User Roles Properties** dialog box.  
If a user assigned to the role you are editing is logged in, a message displays. Click **Yes** to continue. The Management application forces the user to log out.
9. Click **OK** to close the **Server Users** dialog box.

## Removing a user role

---

### NOTE

You must have the User Management privilege to perform this task.

---

You can remove a user role regardless of whether or not a user is assigned to the role. When you remove a role, the role is automatically removed from any resource groups to which it is assigned.

---

### NOTE

When a user assigned to the role you are editing is logged in while you are making changes, the Management application forces the user to log out when you save your work.

---

To remove a role, complete the following steps.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Select the role you want to remove in the **Roles** list.
3. Click **Remove**.
4. Click **Yes** on the confirmation message.  
If a user assigned to the role you are editing is logged in, the Management application forces the user to log out.

5. Click **OK** on the “role removed” message.
6. Click **OK** to close the **Server Users** dialog box.

## Resource groups

The Management application enables you to create resource groups and assign users to the selected role within that group. This enables you to configure user access by both role and fabric when you assign users to a role within the resource group.

### Creating a resource group

#### NOTE

You must have the User Management privilege to perform this task.

The Management application provides one pre-configured resource group (All Fabrics). When you create a resource group, all available roles are automatically assigned to the resource group. Once the resource group is available you can assign a user to a role within the resource group.

To create a resource group, complete the following steps.

1. Select **Server > Users**.

The **Server Users** dialog box displays.

2. Click **Add**.

The **Add/Edit Resource Group** dialog box displays (Figure 146).

| Available Fabrics |          |            |             |
|-------------------|----------|------------|-------------|
| Name              | Location | Contact    | Description |
| Large             | san jose | Uncle Sam. | test        |

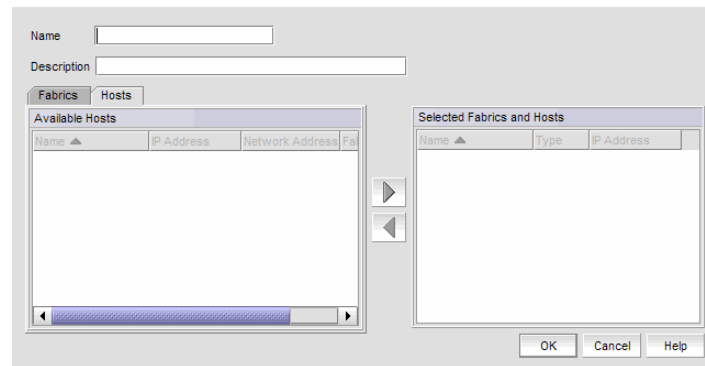
| Selected Fabrics and Hosts |      |            |
|----------------------------|------|------------|
| Name                       | Type | IP Address |

**FIGURE 146** Add/Edit Resource Group dialog box - Fabrics tab

3. Enter a name and description for the group in the fields provided.
4. Click the **Fabrics** tab and complete the following steps to add fabrics to the resource group.
  - a. Select the fabrics you want to include in this group in the **Available Fabrics** table.
  - b. Click the right arrow button.

The selected fabrics are moved to the **Selected Fabrics and Hosts** table.

5. Click the **Hosts** tab and complete the following steps to add hosts to the resource group.



**FIGURE 147** Add/Edit Resource Group dialog box - Hosts tab

- a. Select the hosts you want to include in this group in the **Available Hosts** table.
- b. Click the right arrow button.

The selected fabrics are moved to the **Selected Fabrics and Hosts** table.

6. Click **OK** to save the new resource group and close the **Add/Edit Resource Group** dialog box.

A message box displays indicating the group was created successfully.

7. Click **OK** on the message.

The new resource group displays in the **Resource Groups** list of the **Server Users** dialog box. To add users to this group, follow the instructions in [“Assigning a user to a resource group”](#) on page 361.

8. Click **OK** to close the **Server Users** dialog box.

## Editing a resource group

### NOTE

You cannot edit the default resource group 'All Fabrics'.

To edit a resource group, complete the following steps.

1. Select **Server > Users**.

The **Server Users** dialog box displays.

2. Click **Add**.

The **Add/Edit Resource Group** dialog box displays.

3. Edit the name and description for the group, if necessary.
4. Add fabrics to the resource group by completing the following steps.
  - a. Click the **Fabrics** tab.
  - a. In the **Available Fabrics** table, select the fabrics you want to include in this group.
  - b. Click the right arrow button.

The selected fabrics are moved to the **Selected Fabrics and Hosts** table.

## 14 Removing a resource group

5. Remove fabrics from the resource group by completing the following steps.
  - a. Click the **Fabrics** tab.
  - a. In the **Selected Fabrics and Hosts** table, select the fabrics you want to remove from this group.
  - b. Click the left arrow button.

The selected fabrics are moved to the **Available Fabrics** table.
6. Add hosts to the resource group by completing the following steps.
  - a. Click the **Hosts** tab.
  - a. In the **Available Hosts** table, select the hosts you want to include in this group.
  - b. Click the right arrow button.

The selected hosts are moved to the **Selected Fabrics and Hosts** table.
7. Remove hosts from the resource group by completing the following steps.
  - a. Click the **Hosts** tab.
  - b. In the **Selected Fabrics and Hosts** table, select the hosts you want to remove from this group.
  - c. Click the left arrow button.

The selected hosts are moved to the **Available Hosts** table.
8. Click **OK** to save the resource group and close the **Add/Edit Resource Group** dialog box.

A message box displays indicating the group was updated successfully.
9. Click **OK** on the message.

To add users to this group, follow the instructions in [“Assigning a user to a resource group”](#) on page 361.
10. Click **OK** to close the **Server Users** dialog box.

### Removing a resource group

To remove a resource group, complete the following steps.

1. Select **Server > Users**.

The **Server Users** dialog box displays.
2. Select the resource group you want to remove in the **Resource Groups** table.
3. Click **Remove**.

A message box displays asking you to confirm the removal.

4. Click **Yes** on the message.  
A message box displays indicating the group was removed successfully.
5. Click **OK** on the message.  
The **Server Users** dialog box displays and the resource group no longer displays in the **Resource Groups** list.
6. Click **OK** to close the **Server Users** dialog box.

## Assigning a user to a resource group

---

### NOTE

You must have the User Management privilege to perform this task.

---

You can assign users to a role under a resource group to give permissions for features and topology views. An individual user can only belong to one resource group. To assign a user to a resource group role, complete the following steps.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Select the user you want to assign in the **Users** list.
3. Select the resource group role to which you want to assign the user in the **Resource Groups** list.
4. Click the right arrow button.

The user is assigned to the selected resource group.

---

### NOTE

The user can only manage the Fabrics and Hosts in the selected resource group. To provide access to all fabrics, assign the user to the All Fabrics resource group.

---

---

### NOTE

For Virtual Fabrics, to provide access to the **Logical Switches** dialog box, you must assign the user to the All Fabrics resource group.

---

5. Click **OK** on the **Server Users** dialog box to save your changes and close the dialog box.

---

### NOTE

If you try to add, edit, or remove a Role or Resource Group before you save the user assignment, your work will be lost.

---

### Removing a user from a resource group

---

**NOTE**

You must have the User Management privilege to perform this task.

---

---

**NOTE**

You cannot remove the default resource group 'All Fabrics'.

---

You can remove users from a resource group to take away permissions for features and topology views.

---

---

**NOTE**

If users are logged in when you reassign their group, they are immediately logged out.

---

To remove a user from a resource group, complete the following steps.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Select the user you want to remove in the **Resource Groups** list.  
Press **CTRL** and click to make multiple selections.
3. Click the left arrow button.  
The user is removed from the selected resource group.
4. Click **OK** on the **Server Users** dialog box to save your changes and close the dialog box.

---

**NOTE**

If you try to add, edit, or remove a Role or Resource Group before you save the user removal, your work will be lost.

---

### Finding a user's resource group

---

**NOTE**

Any user with User Management read-only or read-write privilege can find a user's group.

---

You can determine the group to which a user belongs through the **Server Users** dialog box.

1. Select **Server > Users**.  
The **Server Users** dialog box displays.
2. Select a user from the **Users** list.
3. Click **Find**.  
The group to which the user belongs are highlighted in the **Groups** list.
4. Click **OK** to close the dialog box.

# Host management

---

## In this chapter

|                                          |     |
|------------------------------------------|-----|
| • About host management . . . . .        | 363 |
| • HCM software . . . . .                 | 364 |
| • Host discovery . . . . .               | 367 |
| • Connectivity map . . . . .             | 367 |
| • View management . . . . .              | 368 |
| • Host port mapping . . . . .            | 368 |
| • Role-based access control . . . . .    | 369 |
| • Host performance management . . . . .  | 370 |
| • Host fault management . . . . .        | 371 |
| • Host security authentication . . . . . | 373 |
| • supportSave on adapters . . . . .      | 374 |

## About host management

Extensive management operations are supported on the switches and fabrics of the SAN using the Management application. Adapters and hosts are visible as part of the fabrics managed by the Management application. The management operations that are currently available using the Management application are discussed in this chapter.

The Management application integrates with another manageability application called the Host Connectivity Manager (HCM) to provide complete management of the host bus adapters (HBAs) and converged network adapters (CNAs).

- The Management application focuses on operations such as fault management, performance management, and configuration management for multiple adapters and adapter ports and security configuration using Fibre Channel Security Protocol (FC-SP) that is set up on the adapter port and the switch.
- HCM supports management for individual adapters (1/4/8 Gbps HBAs) and 10 Gbps CNAs and other devices, such as the host, CEE ports, FCoE ports, and Ethernet ports.

The Management application, in conjunction with HCM, provides end-to-end management capability. For information about configuring, monitoring, and managing individual adapters using the HCM GUI or the Brocade Command Utility (BCU), refer to the *Brocade Adapters Administrator's Guide*.

## HCM software

The Host Connectivity Manager (HCM) is a management software application for configuring, monitoring, and troubleshooting Brocade host bus adapters (HBAs), converged network adapters (CNAs), and FC mezzanine cards in a storage area network (SAN) environment.

### HCM features

Common HBA and CNA management software features include the following:

- Discovery using the agent software running on the servers attached to the SAN, which enables you to contact the devices in your SAN.
- Configuration management, which enables you to configure local and remote systems. With HCM you can configure the following items:
  - Local host
  - Brocade 4 Gbps and 8 Gbps HBAs
  - HBA ports (including logical ports, base ports, remote ports, and virtual ports)
  - Brocade 10 Gbps single-port and 10 Gbps dual-port converged network adapters (CNAs)
  - CEE ports
  - FCoE ports (CNA only)
  - Ethernet ports (CNA only)
- Diagnostics, which enables you to test the adapters and the devices to which they are connected:
  - Link status of each adapter and its attached devices
  - Loopback test, which is external to the adapter, to evaluate the ports (transmit and receive transceivers) and the error rate on the adapter
  - Read/write buffer test, which tests the link between the adapter and its devices
  - FC protocol tests, including echo, ping, and traceroute
- Monitoring, which provides statistics for the SAN components.
- Security, which enables you to specify a CHAP secret and configure authentication parameters.
- Event notifications, which provide asynchronous notification of various conditions and problems through a user-defined event filter.

## Host bus adapters

Brocade offers five models of Fibre Channel Host Bus Adapters (HBAs). These models provide reliable, high-performance host connectivity for mission-critical SAN environments. The Brocade HBAs are listed in [Table 18](#).

**TABLE 18** Brocade Fibre Channel HBA models

| Model Number | Description                                                                                                                                      | Number of Ports |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Brocade 804  | Dual-port mezzanine HBA with a per-port maximum of 8 Gbps. This HBA installs in server blades that install in supported blade system enclosures. | 2               |
| Brocade 825  | Dual-port stand-up HBA with a per-port maximum of 8 Gbps using a 8 Gbps SFP+. <sup>1</sup>                                                       | 2               |
| Brocade 815  | Single-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP+. <sup>1</sup>                                                     | 1               |
| Brocade 425  | Dual-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP. <sup>2</sup>                                                        | 2               |
| Brocade 415  | Single-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP. <sup>2</sup>                                                      | 1               |

<sup>1</sup> A 4 Gbps SFP installed in Brocade 815 or 825 HBAs allows 4, 2, or 1 Gbps speed only.

<sup>2</sup> An 8 Gbps SFP+ installed in Brocade 425 or 415 HBAs allows 2 or 4 Gbps speed only.

Using Brocade HBAs, you can connect your server (host system) to devices on the Fibre Channel SAN. The combined high performance and proven reliability of a single-ASIC design makes these HBAs ideal for connecting hosts to SAN fabrics based on Brocade Fabric or M-Enterprise operating systems.

### NOTE

The Brocade 804 mezzanine card and Brocade 1007 CNA expansion card connects to the embedded switch modules or embedded interconnect modules on the Blade System chassis by way of an internal backplane and, therefore, no optical modules (SFPs) are involved. With the exception of no SFPs, the Brocade 804 mezzanine FC HBA card and Brocade 1007 CNA expansion card functions the same as the other Brocade adapters.

## Converged network adapters

Table 19 describes available Brocade Converged Network Adapters (CNAs) for PCIe x 8 host bus interfaces, hereafter referred to as Brocade CNAs. These adapters provide reliable, high-performance host connectivity for mission-critical SAN environments.

**TABLE 19** Brocade Fibre Channel CNA Models

| Model Number              | Port Speed      | Number of Ports | Adapter Type |
|---------------------------|-----------------|-----------------|--------------|
| Brocade 1007 <sup>1</sup> | 10 Gbps maximum | 2               | Expansion    |
| Brocade 1020              | 10 Gbps maximum | 2               | Stand-up     |
| Brocade 1010              | 10 Gbps maximum | 1               | Stand-up     |

<sup>1</sup>The Brocade 1007 is a two-port CNA mezzanine or expansion card adapter that mounts on a blade server that installs in a blade system enclosure. The adapter uses FCoE to converge standard data and storage networking data onto a shared Ethernet link. Ethernet and Fibre Channel communication are routed through the CEE ports on the adapter to the blade system enclosure midplane and onto the installed switch modules installed in the enclosure.

For information on installing the Brocade 1007 CNA on a blade server, refer to the *Brocade Adapters Installation and Reference Guide*.

Brocade CNAs combine the functions of a Host Bus Adapter (HBA) and Network Interface Card (NIC) on one PCIe x8 card. The CNAs even appear as network adapters (NIC) and Fibre Channel adapters to the host. These CNAs fully support FCoE protocols and allow Fibre Channel traffic to converge onto 10 Gbps Converged Enhanced Ethernet (CEE) networks. FCoE and 10 Gbps CEE operations are simultaneous.

## Host discovery

The Management application enables you to discover individual hosts, import a group of hosts from a CSV file, or import host names from discovered fabrics. The maximum number of host discovery requests that can be accepted is 1000. Host discovery requires HCM Agent 2.0 or later. SMI and WMI discovery are not supported.

---

**NOTE**

Pure Fabric discovery alone shows adapters behind Access Gateway and all adapter ports as virtual. When you discover an adapter and ports using Host discovery, the adapter and all its ports are shown as physical.

---

Instructions for discovering hosts are detailed in [Chapter 2, “Discovery”](#) and include information about the following:

- [“Discovering Hosts by IP address or hostname”](#) on page 42
- [“Importing Hosts from a CSV file”](#) on page 43
- [“Importing Hosts from a Fabric”](#) on page 44
- [“Configuring Brocade HBA credentials”](#) on page 45
- [“Configuring virtual machine credentials”](#) on page 46
- [“Editing Host credentials”](#) on page 47
- [“Removing a Host from Discovery”](#) on page 48
- [“Viewing the discovery state”](#) on page 48
- [“Troubleshooting discovery”](#) on page 49

## Connectivity map

The Connectivity Map, which displays in the upper right area of the main window, is a grouped map that shows physical and logical connectivity of SAN components, including discovered and monitored devices and connections. These components display as icons in the Connectivity Map. For a list of icons that display in the Connectivity Map, refer to the following tables in [Chapter 1, “Getting Started”](#):

- [“Product icons”](#) on page 11
- [“Group icons”](#) on page 12
- [“Port icons”](#) on page 12

The Management application displays all discovered fabrics in the Connectivity Map by default. To display a discovered Host in the Connectivity Map, you must select the Host in the Product List. You can only view one Host and physical and logical connections at a time.

## View management

You can customize the topology by creating views at the managed host level in addition to the fabric level views. If you discover or import a Fabric with more than approximately 2000 devices, the devices display on the Product List, but not on the Connectivity Map. Instead, the topology area shows a message stating that the topology cannot be displayed. To resolve this issue, create a new view to filter the number of devices being discovered.

Instructions for managing customized views of the topology are detailed in [Chapter 5, “View management”](#) and include information about the following:

## Host port mapping

Host bus adapters (HBAs) and hosts discovered through one or more fabrics can be easily identified in the topology by their product icons. For a list of products and their icons, refer to [“Product icons”](#) on page 11. Once identified in the topology, you can create hosts and assign the HBAs to them and import an externally created host port mapping file (.CSV) to the Management application.

---

### NOTE

The Management application now enables you to map HBAs from multiple fabrics (previous versions limited HBA mapping to one fabric).

---

The Management application also enables you to discover hosts directly using Host discovery (for step-by-step instructions, refer to [“Host discovery”](#) on page 42). If you discover a host directly, when you open the **Host Port Mapping** dialog box, the Management application automatically groups all HBAs under the host.

If you create a new Host and associate HBAs to it, and then you try to discover a host with the same HBAs using Host discovery, the HBA's discovered using host discovery must match the HBAs associated to the Host exactly; otherwise, Host discovery will fail.

Instructions for mapping a Host to HBAs are detailed in [“Host port mapping”](#) in [Chapter 8, “Device Configuration”](#) and include information about the following:

- [“Creating a new Host”](#) on page 201
- [“Renaming an HBA Host”](#) on page 202
- [“Deleting an HBA Host”](#) on page 202
- [“Viewing Host properties”](#) on page 202
- [“Associating an HBA with a Host”](#) on page 203
- [“Importing HBA-to-Host mapping”](#) on page 203
- [“Removing an HBA from a Host”](#) on page 204
- [“Exporting Host port mapping”](#) on page 205

## Role-based access control

The Management application enables you to create resource groups and assign users to the selected role within that group. This enables you to assign users to a role within the resource group.

The Management application provides one pre-configured resource group (All Fabrics). When you create a resource group, all available roles are automatically assigned to the resource group. Once the resource group is available you can assign a user to a role within the resource group.

### Host management privileges

You can launch the Host Connectivity Manager (HCM) if you have read and write permissions to the Host Management privilege. Other HBA-related operations are controlled by the following privileges:

- The HBA technical support launch point is controlled by the Technical Support Data Collection privilege.
- The Fibre Channel Security Protocol (FCSP) launch point is controlled by the Security privilege. Read write (RW) and read only (RO) permissions are required.
- The HBA performance monitoring launch point is controlled by the Performance privilege.

### Host administrator privileges

The Host Administrator role has the following privileges:

- Add and delete properties
- Discovery setup
- Host management
- Performance
- Properties edit
- Security
- Servers
- View management

Instructions for managing resource groups and users using roles and privileges are detailed in [“Users,” “Roles,” and “Resource groups” in Chapter 14, “Role-Based Access Control”](#).

## Host performance management

Real-time performance enables you to collect data from managed HBA and CNA ports. You can use real-time performance to configure the following options:

- Select the polling rate from 20 seconds up to 1 minute.
- Select up to 32 ports total from a maximum of 10 devices for graphing performance.
- Choose to display the same Y-axis range for both the Tx MB/Sec and Rx MB/Sec measure types for easier comparison of graphs.

Table 20 lists the counters that are supported for the FC ports and for the HBA and CNA ports.

**TABLE 20** Counters

| FC port measures      | HBA port measures                  | CNA port measures               |
|-----------------------|------------------------------------|---------------------------------|
| Tx % utilization      | Tx % utilization                   | Tx % utilization                |
| Rx % utilization      | Rx % utilization                   | Rx % utilization                |
| Tx MBps               | Tx MBps                            | Tx MBps                         |
| Rx MBps               | Rx MBps                            | Rx MBps                         |
| CRC errors            | CRC errors                         |                                 |
| Signal losses         | Signal losses                      |                                 |
| Sync losses           | Sync losses                        |                                 |
| Link failures         | Link failures                      |                                 |
| Sequence errors       | Primitive sequence protocol errors |                                 |
| Invalid transmissions |                                    |                                 |
| Rx link resets        |                                    |                                 |
| Tx link resets        |                                    |                                 |
|                       | NOS count                          |                                 |
|                       | Error frames                       |                                 |
|                       | Dropped frames                     |                                 |
|                       | Undersized frames                  |                                 |
|                       | Oversized frames                   |                                 |
|                       | Bad EOF frames                     |                                 |
|                       | Invalid ordered sets               |                                 |
|                       | Non-frame coding error             |                                 |
|                       |                                    | Received paused frames          |
|                       |                                    | Transmitted paused frames       |
|                       |                                    | Received FCoE pause frames      |
|                       |                                    | Transmitted FCoE pause frames   |
|                       |                                    | Received FCS error frames       |
|                       |                                    | Transmitted FCS error frames    |
|                       |                                    | Received alignment error frames |

**TABLE 20** Counters (Continued)

| FC port measures | HBA port measures | CNA port measures            |
|------------------|-------------------|------------------------------|
|                  |                   | Received length error frames |
|                  |                   | Received code error frames   |

Instructions for generating real-time performance data are detailed in [“Generating a real-time performance graph”](#) on page 294.

## Host fault management

Fault management enables you to monitor your SAN using the following methods:

- Monitor logs for specified conditions and notify you or run a script when the specified condition is met.
- Create event-based policies, which contain an event trigger and action.
- Configure E-mail event notification.
- Receive and forward Syslog messages from Fabric OS switches and Brocade HBAs, managed using the Host Connectivity Manager (HCM).

### Adapter events

You can configure triggers and actions for the following event types that are:

- Product Audit Event — occurs when a target product is audited.
- Product Status Event — occurs when a device or connection changes to Up or Down.
- Product Threshold Alert Event — notifies you when a threshold alert has been reached.

You can configure event policies for events you want to monitor. A policy is the mechanism defined by you that identifies the response to specific event types. You can customize the event management policy using triggers and actions, which are explained in [Chapter 10, “Fault Management”](#).

### Event policies

You can create policies for events you want to monitor. A policy is the mechanism defined by you that identifies the response to specific event types. You can customize the event management policy using triggers and actions, which are explained [“Event policies”](#) on page 257. This section also provides information about the following topics:

## Filtering event notifications

The application provides notification of many different types of SAN events. If a user wants to receive notification of certain events, you can filter the events specifically for that user.

---

### NOTE

The e-mail filter in the Management application is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box. See [“Setting up advanced event filtering for the Master Log”](#) on page 254 for more information.

---

To configure event notifications, use the instructions in [“Configuring e-mail notification”](#) on page 274.

## Syslog forwarding

---

### NOTE

Syslog messages are only available on Fabric OS devices and Brocade HBAs (managed using the HCM Agent).

---

Syslog forwarding is the process by which you can configure the Management application to send Syslog messages to other computers. Switches only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you must configure the Management application to listen on a different port. Then you must configure another Syslog server to listen for Syslog messages and forward the messages to the Management application Syslog listening port. Brocade HBAs only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you the management application cannot send Syslog messages to another computer.

Syslog messages are persisted in the database. You can view the Syslog messages from the Management application. However, the Management application does not convert the Syslog messages into event objects except for the audit syslog messages.

For more information about Syslog forwarding, refer to [“Syslog forwarding”](#) on page 283.

# Host security authentication

Fibre Channel Security Protocol (FC-SP) is a mechanism used to secure communication between two switches or between a switch and a device such as an HBA port.

You can use either the Management application or the HCM GUI to display the authentication settings and status. When you enable FC-SP authentication using the Management application, you can also set the authentication settings on the attached 24 - 8 Gbps FC Port, 8 - 10 Gbps CEE Port switch.

**NOTE**

FC-SP is only available for Brocade HBAs that are managed using the HCM agent. FC-SP is not available for virtual ports or unmanaged HBA ports. The user must have the Security privilege to use this feature.

## Configuring security authentication using the Management application

Access the **Fibre Channel Security Protocol Configuration** (FCSP) dialog box by selecting an adapter port from the device tree.

1. Select the appropriate device based on how you want to configure security authentication:
2. Right-click the HCM HBA port and select the **FC Security Protocol** menu item.

The **Fibre Channel Security Protocol Configuration** (adapter level) dialog box displays. The **Fibre Channel Security Protocol Configuration** dialog at the host level displays.

☐ Enable Authentication

|                                                      | Local Port Settings | Attached Switch Settings |
|------------------------------------------------------|---------------------|--------------------------|
| Hash Type                                            | MD5                 |                          |
| DH-Group Type                                        | DHNULL              |                          |
| Secret                                               |                     |                          |
| Confirm Secret                                       |                     |                          |
| <input type="checkbox"/> Also set on attached switch |                     |                          |
|                                                      |                     | OK Cancel Help           |

FIGURE 148 Fibre Channel Security Protocol Configuration - host level dialog box

3. Configure the following parameters on the **FCSP Authentication** dialog box:
  - a. Select the **Enable Authentication** check box to enable or disable the authentication policy.  
 If authentication is enabled, the port attempts to negotiate with the switch. If the switch does not participate in the authentication process, the port skips the authentication process.  
 The Hash type list shows the following options, but only one option, DHNULL, is supported.
    - **MD5** - A hashing algorithm that verifies a message's integrity using Message Digest version 5. MD5 produces a 128-bit digest and is the required authentication mechanism for LDAP v3 servers.
    - **SHA1** - A secure hashing algorithm that computes a 160-bit message digest for a data file that is provided as input.
    - **MD5SHA1** - Similar to the MD5 hashing algorithm, but used for DH-CHAP authentication.
    - **SHA1MD5** - Similar to the SHA1 hashing algorithm, but used for DH-CHAP authentication.
  - b. Select **DHNULL** as the DH-group type value.
  - c. Type and retype the secret.  
 The length of the secret must be between eight and 41 characters and the secret field cannot be blank.
  - d. Select the **Also set on attached switch** check box to set or not set the CHAP secret on the attached switch.
4. Click **OK** to save the changes and close the dialog box.  
 FC Security Protocol settings are also applied to the attached switch.

## supportSave on adapters

Host management features support capturing support information for managed Brocade adapters, which are discovered in the Management application. You can trigger supportSave for multiple adapters at the same time.

You can use Technical Support to collect supportSave data (such as, RASLOG, TRACE and so on) and switch events from Fabric OS devices.

The switch must be running Fabric OS 5.2.X or later to collect technical support data. In addition, you must have the supportSave privilege to collect supportSave information.

---

### NOTE

You cannot schedule Host supportSave information

---

Instructions for scheduling and capturing technical support files are detailed in [“Scheduling technical support information collection”](#) on page 230.

# Fibre Channel over IP

---

## In this chapter

|                                                                             |     |
|-----------------------------------------------------------------------------|-----|
| • FCIP services licensing .....                                             | 376 |
| • FCIP Concepts .....                                                       | 376 |
| • IP network considerations.....                                            | 376 |
| • FCIP platforms and supported features.....                                | 377 |
| • FCIP trunking .....                                                       | 379 |
| • IPsec and IKE implementation over FCIP.....                               | 384 |
| • Open systems tape pipelining.....                                         | 388 |
| • FICON emulation features.....                                             | 389 |
| • FCIP configuration guidelines.....                                        | 390 |
| • Configuring an FCIP tunnel.....                                           | 391 |
| • Adding an FCIP circuit .....                                              | 393 |
| • Use TCP/IP DSCP or L2CoS to prioritize FC traffic.....                    | 394 |
| • Configuring FCIP tunnel advanced settings.....                            | 396 |
| • Viewing FCIP connection properties.....                                   | 401 |
| • Viewing General FCIP properties .....                                     | 402 |
| • Viewing FCIP FC port properties .....                                     | 403 |
| • Viewing FCIP Ethernet port properties.....                                | 404 |
| • Editing FCIP tunnels .....                                                | 405 |
| • Editing FCIP circuits.....                                                | 406 |
| • Disabling FCIP tunnels .....                                              | 407 |
| • Enabling FCIP tunnels.....                                                | 407 |
| • Deleting FCIP tunnels .....                                               | 408 |
| • Displaying FCIP performance graphs.....                                   | 409 |
| • Displaying FCIP performance graphs for Ethernet ports .....               | 409 |
| • Displaying tunnel properties from the FCIP tunnels dialog box.....        | 410 |
| • Displaying FCIP circuit properties from the FCIP tunnels dialog box ..... | 411 |
| • Displaying switch properties from the FCIP Tunnels dialog box.....        | 412 |
| • Displaying fabric properties from the FCIP Tunnels dialog box .....       | 413 |
| • Troubleshooting FCIP Ethernet connections .....                           | 414 |

## FCIP services licensing

Most of the FCIP extension services described in this chapter require the High Performance Extension over FCIP/FC license. FICON emulation features require additional licenses. Use the **licenseShow** command to verify the needed licenses are present on the hardware used on both ends the FCIP tunnel.

## FCIP Concepts

Fibre Channel over IP (FCIP) is a tunneling protocol that enables you to connect Fibre Channel SANs over IP-based networks. Fabric OS extension switches and extension blades use FCIP to encapsulate Fibre Channel frames within IP frames that can be sent over an IP network to a partner Fabric OS extension switch or extension blade. When the IP packets are received, the Fibre Channel frames are reconstructed. FCIP uses a TCP transport that guarantees in-order delivery. The Fibre Channel fabric and all Fibre Channel targets and initiators are unaware of the presence of the IP network.

Because an FCIP tunnel uses an existing IP network, configuring and managing an FCIP tunnel requires knowledge of general IP networking concepts, and specific knowledge about the IP network that will be used for the tunnel. Because the IP network may be used to transport data over very long distances, and because the IP network is not designed exclusively for large data transfers, latency is an issue. Features such as data compression, trunking, Adaptive Rate Limiting (ARL), and Open Systems Tape Pipelining (OSTP) can reduce latency, and help manage tunnel bandwidth more effectively.

## IP network considerations

Because FCIP uses TCP connections over an existing IP network, consult with the IP network administrator to be sure that the network hardware and software equipment operating in the data path can support those connections. Routers and firewalls that are in the data path need to be configured to pass layer 3 protocols 0800 (IP), 0806 (ARP), and 0001 (ICMP). Also, process layer ports for FTP (ports 20 and 21) Telnet (port 23), and SNMP (ports 161 and 162) should be configured on the management IP network to enable support personnel to access and transmit troubleshooting information.

## FCIP platforms and supported features

There are five Fabric OS platforms that support FCIP:

- The 8 Gbps 16-FC ports, 6-Gbps ports extension switch.
- The 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade (384-port Backbone Chassis, 192-port Backbone Chassis).
- The 4 Gbps Extension Switch.
- The 4 Gbps Router, Extension switch.
- The 4 Gbps Router, Extension blade (384-port Backbone Chassis, 192-port Backbone Chassis, Director Chassis).

There are differences in platform capabilities. For example, the 4 Gbps Router, Extension switch, and the 4 Gbps Router, Extension blade cannot support FCIP trunking, and some features, such as support for IPSec and IPv6 addresses, are not currently available for the 8 Gbps 16-FC ports, 6-Gbps ports extension switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade in Fabric OS version 6.3.0, but are planned for a later version. [Table 21](#) summarizes FCIP capabilities per platform.

**TABLE 21** FCIP capabilities

| Capabilities                                                                                                                        | 8 Gbps 16-FC ports, 6-Gbps ports extension switch | 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade | 4 Gbps Router, Extension Switch | 4 Gbps Router, Extension blade |
|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------------------------------------------|---------------------------------|--------------------------------|
| FCIP trunking                                                                                                                       | Yes                                               | Yes                                                   | No                              | No                             |
| Adaptive Rate Limiting                                                                                                              | Yes                                               | Yes                                                   | No                              | No                             |
| 10 GbE ports                                                                                                                        | No                                                | Yes                                                   | No                              | No                             |
| FC ports up to 8 Gbps                                                                                                               | Yes                                               | Yes                                                   | No                              | No                             |
| Compression                                                                                                                         | Yes                                               | Yes                                                   | Yes                             | Yes                            |
| Open Systems Tape Pipelining (OSTP) <ul style="list-style-type: none"> <li>• FCIP Fastwrite</li> <li>• Tape Acceleration</li> </ul> | Yes                                               | Yes                                                   | Yes                             | Yes                            |
| FICON extension                                                                                                                     | Yes                                               | Yes                                                   | Yes                             | Yes                            |
| IPSec for tunnel traffic                                                                                                            | Yes                                               | Yes                                                   | Yes                             | Yes                            |
| Diffserv priorities                                                                                                                 | Yes                                               | Yes                                                   | Yes                             | Yes                            |
| VLAN tagging                                                                                                                        | Yes                                               | Yes                                                   | Yes                             | Yes                            |
| VEX_Ports                                                                                                                           | Yes                                               | Yes                                                   | Yes                             | Yes                            |
| Support for third party WAN optimization hardware                                                                                   | No*                                               | No*                                                   | Yes                             | Yes                            |
| IPv6 addresses for FCIP tunnels                                                                                                     | Yes                                               | Yes                                                   | Yes                             | Yes                            |

\* Support is planned for a later release.

The way FCIP tunnels and virtual ports map to the physical GbE ports depends on the switch or blade model. The 8 Gbps 16-FC ports, 6-Gbps ports extension switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade tunnels are not tied to a specific GbE port, and may be assigned to any virtual port within the allowed range. The 4 Gbps Router, Extension switch and 4 Gbps Router, Extension blade require tunnels to be mapped to specific GbE ports and specific virtual ports. The mapping of GbE ports to tunnels and virtual port numbers is summarized in [Table 22](#).

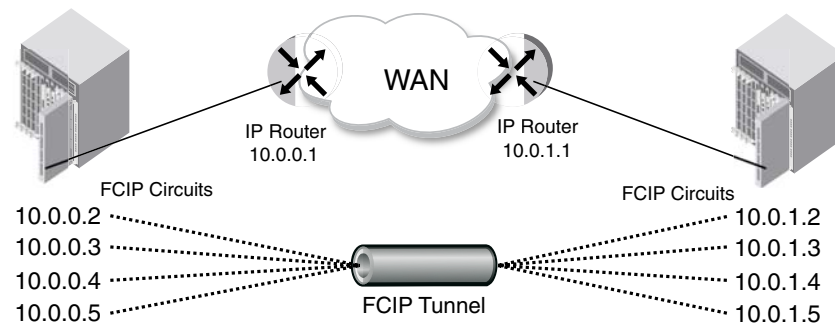
**TABLE 22** GbE port mapping

| Switch or Blade Model                                 | GbE ports                           | Tunnels | Virtual ports (VE_Ports, VEX_Ports)                             |
|-------------------------------------------------------|-------------------------------------|---------|-----------------------------------------------------------------|
| 8 Gbps 16-FC ports, 6-Gbps ports extension switch     | GbE ports 0-5                       | 0-8     | 16-23                                                           |
| 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports blade | GbE ports 0-9<br>10GbE ports 10, 11 | 0-20    | 12-21 used by GbE ports (0-9) and by XGE1<br>24-31 used by XGE0 |
| 4 Gbps Router, Extension switch and blade             | ge0                                 | 0       | 16                                                              |
|                                                       |                                     | 1       | 17                                                              |
|                                                       |                                     | 2       | 18                                                              |
|                                                       |                                     | 3       | 19                                                              |
|                                                       |                                     | 4       | 20                                                              |
|                                                       |                                     | 5       | 21                                                              |
|                                                       |                                     | 6       | 22                                                              |
|                                                       |                                     | 7       | 23                                                              |
|                                                       | ge1                                 | 0       | 24                                                              |
|                                                       |                                     | 1       | 25                                                              |
|                                                       |                                     | 2       | 26                                                              |
|                                                       |                                     | 3       | 27                                                              |
|                                                       |                                     | 4       | 28                                                              |
|                                                       |                                     | 5       | 29                                                              |
|                                                       |                                     | 6       | 30                                                              |
|                                                       |                                     | 7       | 31                                                              |

The 4 Gbps Extension Switch presents only 2 active FC ports and 1 virtual port per GbE interface (ge0 and ge1 in the table above).

## FCIP trunking

FCIP Trunking is a method for managing the use of WAN bandwidth and providing redundant paths over the WAN to protect against transmission loss. This feature is available only on the 8 Gbps extension switches and 8 Gbps extension blades. Trunking is enabled by creating logical circuits within an FCIP tunnel. A tunnel may have multiple circuits. Each circuit is a connection between a pair of IP addresses that are associated with source and destination endpoints of an FCIP tunnel, as shown in [Figure 149](#). Each circuit represents a portion of the available Ethernet bandwidth provided by the GbE ports that are connected to the WAN.



**FIGURE 149** FCIP tunnel and FCIP circuits

## Design for redundancy and fault tolerance

Multiple FCIP tunnels can be defined between pairs of 8 Gbps extension switches and 8 Gbps extension blades, but doing so defeats the concept of a multiple circuit FCIP tunnel. Defining two tunnels between a pair of switches or blades rather than one tunnel with two circuits is not as redundant or fault tolerant as having one multiple circuit tunnel.

## FCIP tunnel restrictions for FCP and FICON emulation features

Multiple FCIP tunnels are not supported between pairs of 8 Gbps extension switches and 8 Gbps extension blades when any of the FICON or FCP emulation features are enabled on the tunnel unless TI Zones or LS/LF configurations are used to provide deterministic flows between the switches. The emulation features require deterministic FC Frame routing between all initiators and devices over multiple tunnels. If there are non-controlled parallel (equal cost) tunnels between the same SID/DID pairs, emulation (Fast Write, Tape Pipelining, XRC or FICON Tape Pipelining) will fail when a command is routed via tunnel 1 and the responses are returned via tunnel 2. Therefore multiple equal cost tunnels are not supported between the switch pairs when emulation is enabled on any one or more tunnels without controlling the routing of SID/DID pairs to individual tunnels using TI Zones or LS/LF configurations.

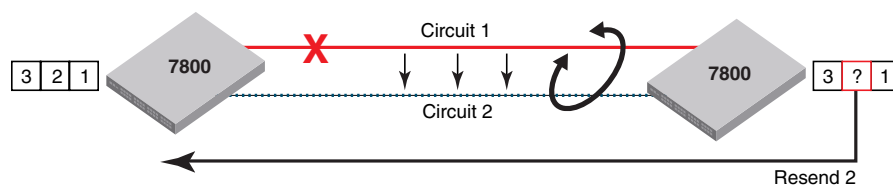
## FCIP Trunk configuration considerations

There are several points to consider when configuring an FCIP trunk:

- Each FCIP circuit is assigned a pair of IP addresses, one source IP address, and one destination IP address.
- The source IP address is used to determine which GbE interface to use. The GbE IP address must be on the same IP subnet as the source IP address. IP subnets cannot span across the GbE interfaces.
- The destination IP address is used to determine routing. If the destination IP address is also on the same subnet as the GbE interface, packets are routed over that subnet. If the destination IP address is on a different subnet, traffic must be routed to an IP gateway address.
- An FCIP circuit can have a maximum commit rate of 1,000,000 Kbps.
- In a scenario where a FCIP tunnel has multiple circuits of different metrics the data will flow over the lower metric circuits unless a failover condition occurs, as described in [“FCIP circuit failover capabilities”](#).
- The maximum bandwidth for a single circuit is 1 Gbps. To utilize the entire bandwidth of an XGE (10GbE) port, you must create ten 1 Gbps circuits.

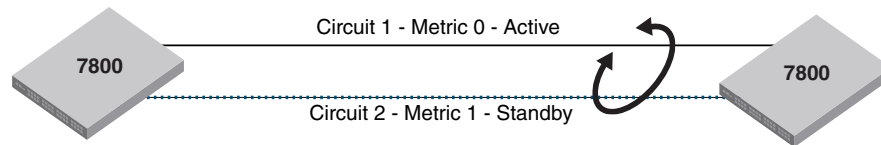
## FCIP circuit failover capabilities

Each FCIP circuit is assigned a metric, which is used in managing failover for FC traffic. Typically, the metric will be either 0 or 1. If a circuit fails, FCIP Trunking tries first to retransmit any pending send traffic over another lowest metric circuit. In [Figure 150](#), circuit 1 and circuit 2 are both lowest metric circuits. Circuit 1 has failed, and transmission fails over to circuit 2, which has the same metric. Traffic that was pending at the time of failure is retransmitted over circuit 2. In order delivery is ensured by the receiving 7800 switch.



**FIGURE 150** Link loss and retransmission over peer lowest metric circuit

In [Figure 151](#), circuit 1 is assigned a metric of 0, and circuit 2 is assigned a metric of 1. In this case, circuit 2 is a standby that is not used unless there are no lowest metric circuits available. If all lowest metric circuits fail, then the pending send traffic is retransmitted over any available circuits with the higher metric,



**FIGURE 151** Failover to a higher metric standby circuit

## Bandwidth calculation during failover

The bandwidth of higher metric circuits is not calculated as available bandwidth on an FCIP tunnel until all lowest metric circuits have failed. For example, assume the following:

- Circuits 0 and 1 are created with a metric of 0. Circuit 0 is created with a maximum transmission rate of 1 Gbps, and Circuit 1 is created with a maximum transmission rate of 500 Mbps. Together, Circuits 0 and 1 provide an available bandwidth of 1.5 Gbps.
- Circuits 2 and 3 are created with a metric of 1. Both are created with a maximum transmission rate of 1 Gbps, for a total of 2 Gbps. This bandwidth is held in reserve.
- If either circuit 0 or circuit 1 fails, traffic flows over the remaining circuit while the failed circuit is being recovered. The available bandwidth is still considered to be 1.5 Gbps.
- If both circuit 0 and circuit 1 fail, there is a failover to circuits 2 and 3, and the available bandwidth is updated as 2 Gbps.
- If a low metric circuit becomes available again, the high metric circuits go back to standby status, and the available bandwidth is updated again. For example, if circuit 0 is recovered, the available bandwidth is updated as 1 Gbps. If circuit 1 is also recovered, the available bandwidth is updated as 1.5 Gbps.

## Adaptive Rate Limiting

Adaptive Rate Limiting (ARL) is performed on FCIP tunnel connections to change the rate in which the FCIP tunnel transmits data through the TCP connections. This feature is available only on the 8 Gbps extension switches and 8 Gbps extension blades. ARL uses information from the TCP connections to determine and adjust the rate limit for the FCIP tunnel dynamically. This allows FCIP connections to utilize the maximum available bandwidth while providing a minimum bandwidth guarantee.

ARL applies a minimum and maximum traffic rate, and allows the traffic demand and WAN connection quality to dynamically determine the rate. As traffic increases, the rate grows towards the maximum rate, and if traffic subsides, the rate reduces towards the minimum. If traffic is flowing error-free over the WAN, the rate grows towards the maximum rate. If TCP reports an increase in retransmissions, the rate reduces towards the minimum.

### FSPF link cost calculation when ARL is used

Fabric Shortest Path First (FSPF) is a link state path selection protocol that directs traffic along the shortest path between the source and destination based upon the link cost. When ARL is used, The link cost is equal to the sum of maximum traffic rates of all established, currently active low metric circuits in the tunnel. The following formulas are used:

- If the bandwidth is greater than or equal to 2 Gbps, the link cost is 500.
- If the bandwidth is less than 2 Gbps, but greater than or equal to 1 Gbps, the link cost is 1000000 divided by the bandwidth.
- If the bandwidth is less than 1 Gbps, the link cost is 2000 minus the bandwidth

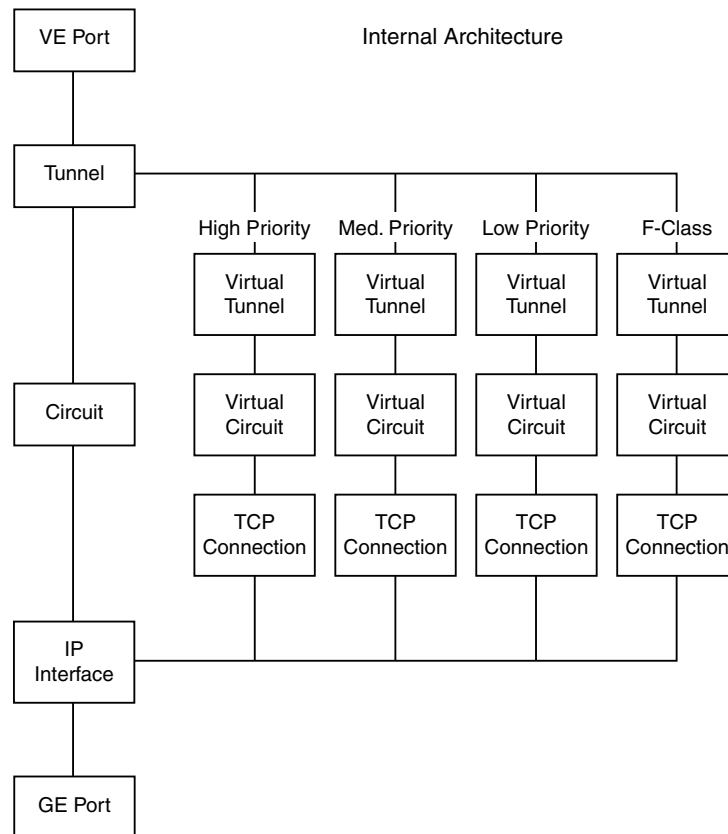
## QoS SID/DID priorities over an FCIP trunk

QoS SID/DID traffic prioritization is a capability of Brocade Fabric OS Adaptive Networking licensed feature. This feature allows you to prioritize FC traffic flows between hosts and targets.

Four internal TCP connections provide internal circuits for managing QoS SID/DID priorities over an FCIP tunnel, as illustrated in [Figure 152](#). The priorities are as follows:

- F class - F class is the highest priority, and is assigned bandwidth as needed at the expense of lower priorities, if necessary.
- QoS high - The QoS high priority gets at least 50% of the available bandwidth.
- QoS medium - The QoS medium priority gets at least 30% of the available bandwidth.
- QoS low - The QoS low priority gets at least 20% of the available bandwidth.

These priorities are enforced only when there is congestion on the network. If there is no congestion, all traffic is handled at the same priority.



**FIGURE 152** TCP connections for handling QoS SID/DID-based FC traffic prioritization

## IPsec and IKE implementation over FCIP

Internet Protocol security (IPsec) uses cryptographic security to ensure private, secure communications over Internet Protocol networks. IPsec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. It helps secure your SAN against network-based attacks from untrusted computers, attacks that can result in the denial-of-service of applications, services, or the network, data corruption, and data and user credential theft. IPsec does not require you to configure separate security for each application that uses TCP/IP.

When configuring for IPsec, however, you must ensure that the same policies are defined in the switches or blades at each end of the FCIP tunnel. IPsec works on FCIP tunnels with or without compression, FCIP Fastwrite, and tape acceleration. IPsec can only be created on tunnels using IPv4 addressing.

### IPsec for the 4 Gbps platforms

IPsec uses some terms that you should be familiar with before beginning your configuration. These are standard terms, but are included here for your convenience.

| Term     | Definition                                                                                                                                                                                                                                                                                                                                 |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AES      | Advanced Encryption Standard. FIPS 197 endorses the Rijndael encryption algorithm as the approved AES for use by US Government organizations and others to protect sensitive information. It replaces DES as the encryption standard.                                                                                                      |
| AES-XCBC | Cipher Block Chaining. A key-dependent one-way hash function (MAC) used with AES in conjunction with the Cipher-Block-Chaining mode of operation, suitable for securing messages of varying lengths, such as IP datagrams.                                                                                                                 |
| AH       | Authentication Header - like ESP, AH provides data integrity, data source authentication, and protection against replay attacks but does not provide confidentiality.                                                                                                                                                                      |
| DES      | Data Encryption Standard is the older encryption algorithm that uses a 56-bit key to encrypt blocks of 64-bit plain text. Because of the relatively shorter key length, it is not a secured algorithm and no longer approved for Federal use.                                                                                              |
| 3DES     | Triple DES is a more secure variant of DES. It uses three different 56-bit keys to encrypt blocks of 64-bit plain text. The algorithm is FIPS-approved for use by Federal agencies.                                                                                                                                                        |
| ESP      | Encapsulating Security Payload is the IPsec protocol that provides confidentiality, data integrity and data source authentication of IP packets, and protection against replay attacks.                                                                                                                                                    |
| IKE      | Internet Key Exchange is defined in RFC 2407, RFC 2408 and RFC 2409. IKEv2 is defined in RFC 4306. IKE uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived and communicating parties are authenticated. The IKE protocol creates a security association (SA) for both parties. |
| MD5      | Message Digest 5, like SHA-1, is a popular one-way hash function used for authentication and data integrity.                                                                                                                                                                                                                               |
| SHA      | Secure Hash Algorithm, like MD5, is a popular one-way hash function used for authentication and data integrity.                                                                                                                                                                                                                            |
| MAC      | Message Authentication Code is a key-dependent, one-way hash function used for generating and verifying authentication data.                                                                                                                                                                                                               |
| HMAC     | A stronger MAC because it is a keyed hash inside a keyed hash.                                                                                                                                                                                                                                                                             |
| SA       | Security Association is the collection of security parameters and authenticated keys that are negotiated between IPsec peers.                                                                                                                                                                                                              |

The following limitations apply to using IPSec:

- IPSec is not supported on 10GbE ports.
- IPSec-specific statistics are not supported.
- To change the configuration of a secure tunnel, you must delete the tunnel and recreate it.
- There is no RAS message support for IPSec.
- IPSec can only be configured on IPv4 based tunnels.
- Secure Tunnels cannot be defined with VLAN Tagged connections.
- For the 4 Gbps Router, Extension switch and blade:
  - IPv6, NAT, and AH are not supported when IPSec is implemented.
  - You can only create a single secure tunnel on a port; you cannot create a nonsecure tunnel on the same port as a secure tunnel.
  - Jumbo frames are not supported.

## IPSec for the 8 Gbps platforms

The 8 Gbps platforms use AES-GCM-ESP as a single, pre-defined mode of operation for protecting all TCP traffic over an FCIP tunnel. AES-GCM-ESP is described in RFC-4106. Key features are listed below:

- Encryption is provided by AES with 256 bit keys.
- The IKEv2 key exchange protocol is used by peer switches and blades for mutual authentication.
- IKEv2 uses UDP port 500 to communicate between the peer switches or blades.
- All IKE traffic is protected using AES-GCM-ESP encryption.
- Authentication requires the generation and configuration of 32 byte pre-shared secrets for each peer switch or blade.
- An SHA-512 hash message authentication code (HMAC) is used to check data integrity and detect third party tampering.
- PRF is used to strengthen security. The PRF algorithm generates output that appears to be random data, using the SHA-512 HMAC as the seed value.
- A 2048 bit Diffie-Hellman (DH) group is used for both IKEv2 and IPSec key generation.
- The SA lifetime limits the length of time a key is used. When the SA lifetime expires, a new key is generated, limiting the amount of time an attacker has to decipher a key. Depending on the length of time expired or the length of the data being transferred, parts of a message maybe protected by different keys generated as the SA lifetime expires. For the 7800 switch and FX8-24 blade, the SA lifetime is approximately eight hours, or two gigabytes of data, whichever occurs first.
- ESP is used as the transport mode. ESP uses a hash algorithm to calculate and verify an authentication value, and also encrypts the IP datagram.

## QoS, DSCP, and VLANs

Quality of Service (QoS) refers to policies for handling differences in data traffic. These policies are based on data characteristics and delivery requirements. For example, ordinary data traffic is tolerant of delays and dropped packets, but voice and video data are not. QoS policies provide a framework for accommodating these differences in data as it passes through a network.

QoS for Fibre Channel traffic is provided through internal QoS priorities. Those priorities can be mapped to TCP/IP network priorities. There are two options for TCP/IP network-based QoS:

- Layer three DiffServ code Points (DSCP).
- VLAN tagging and Layer two class of service (L2CoS).

### DSCP quality of service

Layer three class of service DiffServ Code Points (DSCP) refers to a specific implementation for establishing QoS policies as defined by RFC2475. DSCP uses six bits of the Type of Service (TOS) field in the IP header to establish up to 64 different values to associate with data traffic priority.

DSCP settings are useful only if IP routers are configured to enforce QoS policies uniformly within the network. IP routers use the DSCP value as an index into a Per Hop Behavior (PHB) table. Control connections and data connections may be configured with different DSCP values. Before configuring DSCP settings, determine if the IP network you are using implements PHB, and consult with your WAN administrator to determine the appropriate DSCP values.

### VLANs and layer two quality of service

Devices in physical LANs are constrained by LAN boundaries. They are usually in close proximity to each other, and share the same broadcast and multicast domains. Physical LANs often contain devices and applications that have no logical relationship. Also, when logically related devices and applications reside in separate LAN domains, they must be routed from one domain to the other.

A VLAN is a virtual LAN network. A VLAN may reside within a single physical network, or it may span several physical networks. Related devices and applications that are separated by physical LAN boundaries can reside in the same VLAN. Also, a large physical network can be broken down into smaller VLANs. VLAN traffic is routed using 802.1Q-compliant tags within an Ethernet frame. The tag includes a unique VLAN ID, and Class of Service (CoS) priority bits. The CoS priority scheme (also called Layer two Class of Service or L2CoS), uses three Class of Service (CoS or 802.1P) priority bits, allowing eight priorities. Consult with your WAN administrator to determine usage.

## When both DSCP and L2CoS are used

If an FCIP tunnel or circuit is VLAN tagged, both DSCP and L2CoS are relevant, unless the VLAN is end-to-end, with no intermediate hops in the IP network. The following table shows the default mapping of DSCP priorities to L2Cos priorities. This may be helpful when consulting with the WAN administrator. These values may be modified per FCIP tunnel.

**TABLE 23** Default Mapping of DSCP priorities to L2Cos Priorities

| DSCP priority/bits | L2CoS priority/bits | Assigned to:        |
|--------------------|---------------------|---------------------|
| 46 / 101110        | 7 / 111             | Class F             |
| 7 / 000111         | 1 / 001             | Medium QoS          |
| 11 / 001011        | 3 / 011             | Medium QoS          |
| 15 / 001111        | 3 / 011             | Medium QoS          |
| 19 / 010011        | 3 / 011             | Medium QoS          |
| 23 / 010111        | 3 / 011             | Medium QoS          |
| 27 / 011011        | 0 / 000             | Class 3 Multicast   |
| 31 / 011111        | 0 / 000             | Broadcast/Multicast |
| 35 / 100011        | 0 / 000             | Low QoS             |
| 39 / 100111        | 0 / 000             | Low QoS             |
| 43 / 101011        | 4 / 100             | High QoS            |
| 47 / 101111        | 4 / 100             | High QoS            |
| 51 / 110011        | 4 / 100             | High QoS            |
| 55 / 110111        | 4 / 100             | High QoS            |
| 59 / 111011        | 4 / 100             | High QoS            |
| 63 / 111111        | 0 / 000             | -                   |

## Open systems tape pipelining

Open Systems Tape Pipelining (OSTP) can be used to enhance open systems SCSI tape write I/O performance. To implement OSTP over FCIP, you must enable the following two features:

- FCIP Fastwrite and Tape Acceleration.
- FC Fastwrite.

### FCIP Fastwrite and Tape Acceleration

When the FCIP link is the slowest part of the network, consider using FCIP Fastwrite and Tape Read and Write Pipelining. FCIP Fastwrite and Tape Acceleration are two features that provide accelerated speeds for read and write I/O over FCIP tunnels in some configurations:

- FCIP Fastwrite accelerates the SCSI write I/Os over FCIP.
- Tape Acceleration accelerates SCSI read and write I/Os to sequential devices (such as tape drives) over FCIP, which reduces the number of round-trip times needed to complete the I/O over the IP network and speeds up the process. To use Tape Acceleration, you must also enable FCIP Fastwrite.

Both sides of an FCIP tunnel must have matching configurations for these features to work. FCIP Fastwrite and Tape Acceleration are enabled by turning them on during the tunnel configuration process. They are enabled on a per-FCIP tunnel basis.

Consider the constraints described in [Table](#) when configuring tunnels to use OSTP.

| FCIP Fastwrite                                                                                                                                                                | Tape Acceleration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Each GbE port supports up to 2048 simultaneous accelerated exchanges, which means a <i>total of 2048 simultaneous exchanges combined</i> for Fastwrite and Tape Acceleration. | Each GbE port supports up to 2048 simultaneous accelerated exchanges, which means a <i>total of 2048 simultaneous exchanges combined</i> for Fastwrite and Tape Acceleration.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Does not natively support multiple equal-cost path configurations. Traffic isolation zoning can be used to support these configurations.                                      | Does not natively support multiple equal-cost path configurations or multiple non-equal-cost path configurations. Traffic isolation zoning can be used to support these configurations.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Class 3 traffic is accelerated with Fastwrite.                                                                                                                                | Class 3 traffic is accelerated between host and sequential device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                                                                                                                                                               | With sequential devices (tape drives), there are 1024 initiator-tape (IT) pairs per GbE port, but 2048 initiator-tape-LUN (ITL) pairs per GbE port. The ITL pairs are shared among the IT pairs. For example:<br>Two ITL pairs for each IT pair as long as the target has two LUNs.<br>If a target has 32 LUNs, 32 ITL pairs for IT pairs. In this case, only 64 IT pairs are associated with ITL pairs. The rest of the IT pairs are not associated to any ITL pairs, so no Tape Acceleration is performed for those pairs. By default, only Fastwrite-based acceleration is performed on the unassociated pairs. |
|                                                                                                                                                                               | Does not support multiple non-equal-cost path between host and sequential device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## FICON emulation features

FICON emulation supports FICON traffic over IP WANs using FCIP as the underlying protocol. FICON emulation features support performance enhancements for specific applications. If you are using FCIP for distance extension in a FICON environment, evaluate the need for these features before you run the FCIP configuration wizard. FICON emulation may be configured by selecting **Advanced Settings** on the **Add Tunnel** or **Edit Tunnel** dialogs. The following features are available:

- XRC emulation.
- Tape write pipelining.
- Tape read pipelining.

### XRC emulation

The eXtended Remote Copy (XRC) application is a DASD application that implements disk mirroring, as supported by the disk hardware architecture and a host software component called System Data Mover (SDM). The primary volume and the secondary mirrored volume may be geographically distant across an IP WAN. The latency introduced by greater distance creates delays in anticipated responses to certain commands. The FICON pacing mechanism may interpret delays as an indication of a large data transfer that could monopolize a shared resource, and react by throttling the I/O. XRC emulation provides local responses to remote hosts, eliminating distance related delays. A FICON XRC Emulation License is required to enable XRC Emulation.

### Tape write pipelining

FICON tape write pipelining improves performance for a variety of applications when writing to tape over extended distances. FICON tape write pipelining locally acknowledges write data records, enabling the host to generate more records while previous records are in transit across the IP WAN. If exception status is received from the device, the writing of data and emulation is terminated. The FICON Tape Emulation License is required to enable FICON Tape Write Pipelining.

### Tape read pipelining

FICON tape read pipelining improves performance for certain applications when reading from FICON tape over extended distances. FICON tape read pipelining reads data from tape directly from the tape device. Reading of tape continues until a threshold is reached. The buffered data is forwarded to the host in response to requests from the host. When the host sends the status accept frame indicating that the data was delivered, the read processing on the device side credits the pipeline and requests more data from the tape. If exception status is received from the device, the reading of data and emulation is terminated. The FICON Tape Emulation License is required to enable FICON Tape Read Pipelining.

## FCIP configuration guidelines

FCIP configuration always involves two or more extension switches. The following should take place first before you configure a working FCIP connection from the Management application:

- The WAN link should be provisioned and tested for integrity.
- Cabling within the data center should be completed.
- Equipment should be physically installed and powered on.
- The Management application must have management port access to the extension switches.
- The Management application must be able to discover the fabrics the contain the extension switches.
- The extension switches should be physically connected to the IP network they will be using to pass data, and the connection should be active and working.
- Identify all the devices in the data path between the extension switches, including Ethernet switches, Ethernet routers, firewalls, and common carrier equipment. A network diagram is very helpful. Support engineers may ask you to provide a network diagram when troubleshooting problems.
- Routers and firewalls must be configured to pass ARP, ICMP, and IP layer 3 protocols.
- Persistently disable the VE\_ports before you configure them. Ports on a new extension switch or extension blade are persistently disabled by default.
- Determine which features you are implementing, and gather the information needed to implement those features. [Table 21](#) summarizes feature support per FCIP platform.

### Virtual Port Types

Virtual ports may be defined as VE\_Ports or VEX\_Ports.

#### VE\_Ports

VE\_Ports (virtual E\_Ports) are used to create interswitch links (ISLs) through an FCIP tunnel. If VE\_Ports are used on both ends of an FCIP tunnel, the fabrics connected by the tunnel are merged.

#### VEX\_Port

A VEX\_Port enables FC-FC Routing Service functionality over an FCIP tunnel. VEX\_Ports enable interfabric links (IFLs). If a VEX\_Port is on one end of an FCIP tunnel, the fabrics connected by the tunnel are not merged. The other end of the tunnel must be defined as a VE\_Port.

# Configuring an FCIP tunnel

When you configure an FCIP extension connection, you create FCIP tunnels and FCIP circuits, between two extension switches.

1. Select **Configure > FCIP Tunnels**.

The **FCIP Tunnels** dialog box is displayed (Figure 153). All discovered fabrics with extension switches are listed under devices.

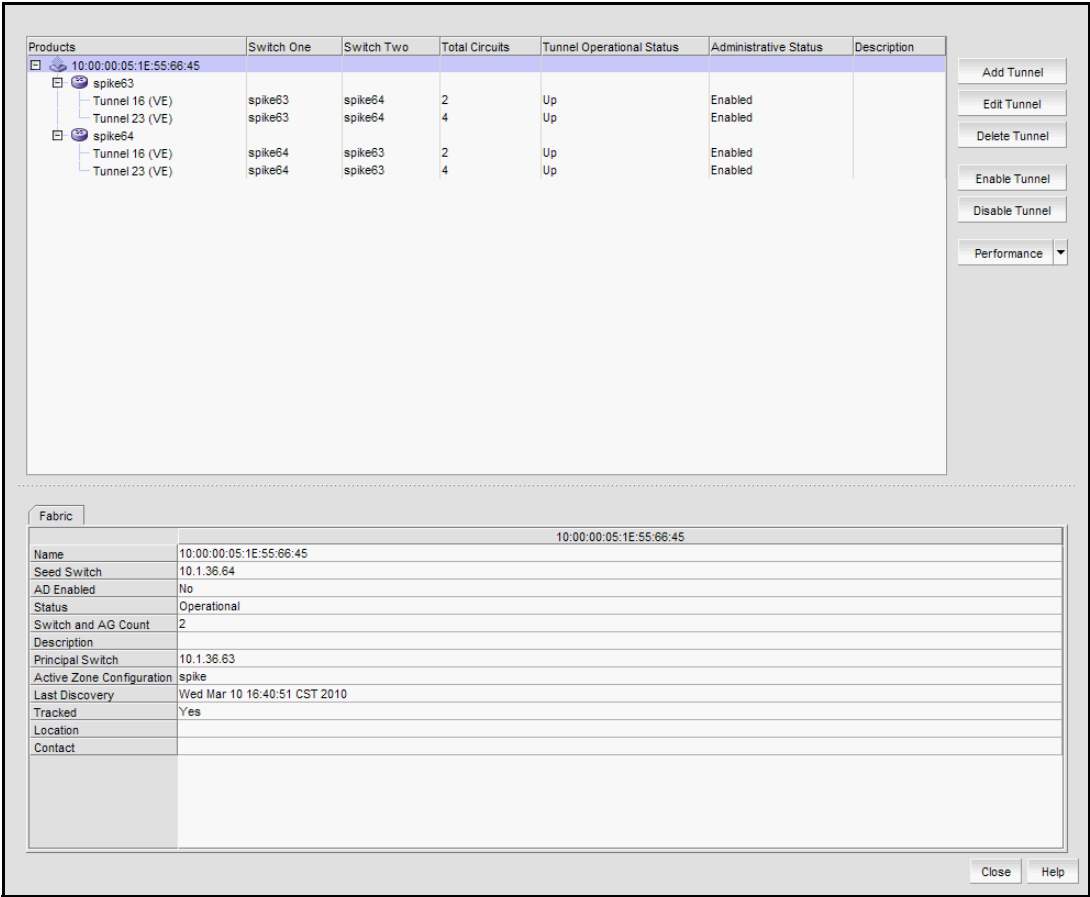


FIGURE 153 FCIP Tunnels dialog box

2. Select the switch you want to configure under **Devices**.

- Click the **Add Tunnel** button, or right-click on the switch and select **Add Tunnel**.

The **Add FCIP Tunnel** dialog is displayed (Figure 154). The name of the switch you selected is displayed in the **Switch** field under **Switch One Settings**. This dialog allows you to configure settings for both switches on either end of the tunnel.

The dialog box is titled "Configure the settings for the tunnel to be added on the selected switch and a second switch if selected. At least one circuit (IP interface) should be set up for adding a tunnel." It is divided into two main sections: "Switch One Settings" and "Switch Two Settings".

**Switch One Settings:**

- Switch:** spike63
- Fabric:** 10:00:00:05:1E:55:66:45
- Tunnel:** 16 (Requires Circuit Configuration)
- Description:** (empty text field)
- Port Type:** ☒ VE Port, ☐ VEX Port
- Fabric ID:** (empty text field)
- Interop Mode:** Brocade (dropdown menu)

**Switch Two Settings:**

- Select Switch Two:** (button)
- Switch:** (empty text field)
- Fabric:** (empty text field)
- Tunnel:** (empty dropdown menu)
- Description:** (empty text field)
- Port Type:** ☒ VE Port, ☐ VEX Port
- Fabric ID:** (empty text field)
- Interop Mode:** Brocade (dropdown menu)

At the bottom left are buttons for "Add Circuit" and "Advanced Settings". At the bottom right are buttons for "OK", "Cancel", and "Help".

**FIGURE 154** Add FCIP Tunnel dialog box

- Click **Select Switch Two** under **Switch Two Settings** to display discovered extension switches, and select the switch that you want to connect to switch one.

The switch name and fabric are displayed in the **Switch** and **Fabric** fields.

- Enter a description of the tunnel in the **Description** field.

#### NOTE

You cannot assign a **Tunnel ID** until after at least one circuit is configured. The **Add Circuit** dialog returns you to the **Add FCIP Tunnel** dialog to allow you to select the **Tunnel ID**.

- Select **Add Circuit**.

The **Add FCIP Circuit** dialog is displayed. Continue with "Adding an FCIP circuit".

## Adding an FCIP circuit

When adding a new FCIP tunnel, you can add an FCIP circuit by selecting the **Add Circuit** button on the **Add FCIP Tunnel** dialog box. Additional FCIP circuits can be added to existing FCIP tunnels by clicking **Add Circuit** from the **Circuit** tab, or by right-clicking on an existing tunnel and selecting **Add Circuit**.

Physical connection between the two tunnel switches is required for suggesting MTU size, maximum bandwidth and verifying IP Connectivity.

Circuit Number

| Switch One Settings                                                                                           | Switch Two Settings                                                    |
|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Switch: <input type="text" value="spike63"/>                                                                  | Switch: <input type="text"/>                                           |
| Fabric: <input type="text" value="10:00:00:05:1E:55:66:45"/>                                                  | Fabric: <input type="text"/>                                           |
| GigE Port: <input type="text" value="ge0"/>                                                                   | GigE Port: <input type="text"/>                                        |
| IP Address Type: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6                             | IP Address Type: <input type="radio"/> IPv4 <input type="radio"/> IPv6 |
| IP Address: <input type="text" value="192.168.0.63"/>                                                         | IP Address: <input type="text"/>                                       |
| Subnet Mask: <input type="text" value="255.255.255.0"/>                                                       | Subnet Mask: <input type="text"/>                                      |
| Default route will get created using the above IP address.                                                    |                                                                        |
| <input type="checkbox"/> Create Non-Default Route                                                             |                                                                        |
| Gateway: <input type="text"/>                                                                                 | Gateway: <input type="text"/>                                          |
| Remote IP Interface: <input type="text"/>                                                                     |                                                                        |
| MTU Size: <input type="text" value="1500"/> (1260 - 1500) <input type="button" value="Suggest"/>              | MTU Size: <input type="text" value="Same as Switch One"/>              |
| Metric: <input type="text" value="0"/>                                                                        | Metric: <input type="text" value="Same as Switch One"/>                |
| VLAN ID: <input type="text"/>                                                                                 | VLAN ID: <input type="text" value="Same as Switch One"/>               |
| (Blank or 1 - 4094, Fabric OS Version >= 6.0.0)                                                               |                                                                        |
| Bandwidth (Mb/s): <input type="radio"/> Uncommitted <input checked="" type="radio"/> Committed (10-1000 Mb/s) |                                                                        |
| Minimum: <input type="text" value="10.0"/> Maximum: <input type="text" value="10.0"/>                         |                                                                        |
| <input type="button" value="Current Maximum Bandwidth"/>                                                      |                                                                        |
| (Requires Physical Connection)                                                                                |                                                                        |
| <input type="button" value="Verify IP Connectivity"/> <input type="button" value="Advanced Settings"/>        |                                                                        |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>   |                                                                        |

**FIGURE 155** Add FCIP Circuit dialog box

1. Select the **GiGE Port** used for the Ethernet connection on each switch. The choices available depend on the extension switch or blade model.
2. Select the **IP Address Type**. The implementation is a dual IP layer operation implementation as described in RFC 4213. IPv6 addresses can exist with IPv4 addresses on the same interface, but the FCIP circuits must be configured as IPv6 to IPv6 and IPv4 to IPv4 connections. IPv6-to-IPv4 connections are not supported. Likewise, encapsulation of IPv4 in IPv6 and IPv6 in IPv4 is not supported.
3. Select the **IP Address** for each port. This implementation of IPv6 uses unicast addresses for the interfaces with FCIP circuits. The unicast address must follow the RFC 4291 IPv6 standard and use the IANA assigned IPv6 Global Unicast address space (2000::/3).

4. For IPv4 addresses, specify the **Subnet Mask**. For IPv6 addresses, specify the prefix length.  
The default is created from the IP address and Subnet Mask. If you want to create a route through a gateway router, click **Create Non-Default Route**, and select a **Gateway address**.
5. Enter the **MTU Size**.  
For SAN traffic, the largest possible MTU (Maximum Transmission Unit) size is generally the most efficient. If you have an active connection between switch one and switch two, click **Suggest** under **Switch One Settings**. To determine a suggested size, packets are sent across the FCIP tunnel, starting at the largest possible size packet that can be sent over IP. If a valid connection response is not received, a smaller packet is sent. This continues until a valid connection response is received, and that size becomes the suggested MTU. MTU settings must match at both ends of the tunnel, and the setting specified under **Switch One Settings** is automatically applied to switch two.
6. If a VLAN ID is used to route frames between the switches over the physical connection, enter the **VLAN ID** under **Switch One Settings**. The same VLAN ID is automatically assigned to switch two. The VLAN ID is an integer value between 1 and 4094 which sets the VLAN tag value in the header assigning the traffic to that specific VLAN. Layer two class of service (L2CoS) values may be assigned to establish traffic priorities over a VLAN. This is done as an **Advanced Setting**.
7. The **Metric** option is used to identify a failover circuit. By assigning a non-zero metric (1), you identify the circuit as a failover circuit. By default, a circuit is assigned a metric of 0. If a circuit fails, FCIP trunking tries first to retransmit any pending send traffic over another circuit with a metric of 0. If no circuits with a metric of 0 are available, then the pending send traffic is retransmitted over any available circuit with a metric of 1.
8. Select values for bandwidth settings. An uncommitted bandwidth is not allowed on an FCIP circuit. You must select **Committed bandwidth**. If you want to use ARL, set **Minimum** and **Maximum** bandwidth values. Bandwidth grows towards the maximum and reduces towards the minimum based on traffic conditions. If you do not want to use ARL, set **Minimum** and **Maximum** to the same value to set a single committed bandwidth. Refer to [“Adaptive Rate Limiting”](#) on page 382 for more information about ARL.
9. If the physical connection exists, click **Verify IP Connectivity** to test the connection between switch one and switch two. The IP connectivity of the connection is tested with the ping utility.
10. Select **Advanced Settings** and continue if you want to do any of the following:
  - Turn selective acknowledgement off.
  - Set the keep alive timeout to a value other than the default of 10 seconds.
  - Set the minimum retransmission time to a value other than the default of 100 ms.
  - Set the maximum retransmits to a value other than the default.
  - Use TCP/IP DSCP or L2CoS to prioritize FC traffic.

If you select **Advanced Settings**, the **Transmission tab** of the **FCIP Circuit Advanced Settings** dialog box displays ([Figure 156](#)).

The screenshot shows the 'Transmission' tab of a configuration window. It includes a 'Selective Ack' checkbox which is checked. Below it are three input fields: 'Keep Alive Time Out (ms)' set to 900, 'Min. Retransmission Time (ms)' set to 100, and 'Max. Retransmits' set to 8. At the bottom, there are four rows of settings for L2Cos and DSCP classes (F-Class, Low, Medium, High), each with a dropdown menu set to 0 and a range in parentheses (0-63). The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

**FIGURE 156 FCIP Circuit Advanced Settings**

- Select the **Selective Ack Off** check box to disable or enable selective acknowledgement. Selective acknowledgement allows a receiver to acknowledge multiple lost packets with a single ACK response. This results in better performance and faster recovery time. Normally, selective acknowledgement should not be disabled. Do not disable selective acknowledgement unless you have a specific need to do so in your operating environment.
- Use the **Keep Alive Time Out (ms)** option to override the default value of 10000 ms. As shown, the range is from 500 to 7200000.
- Use the **Max. Retransmission Time (ms)** option to override the default value of 100 ms.
- Use the **Max. Retransmits** option to override the default value of 8. As shown, the range is 1 to 8.
- Select **L2CoS** and **DSCP** priorities. Refer to “[QOS, DSCP, and VLANs](#)” on page 386 for more information.

11. Click **Finish** to close the **FCIP Tunnel Configuration** wizard.

## Configuring FCIP tunnel advanced settings

Compression, FCIP fast write and tape pipelining, IPSec and IKE policies, and FICON emulation features are configured as advanced settings.

1. Click **Advanced Settings** on the **Add FCIP Tunnel** dialog box.

The **Advanced Settings** dialog box is displayed. This dialog box has a **Transmission** tab, **Security** tab, and **FICON Emulation** tab.

2. Click **OK** to close **Advanced Settings** when you have configured the features that you want to implement.
3. Click **OK** to close the **Add FCIP Tunnel** dialog box.

### Enabling and disabling compression

Data compression can improve performance on long distance connections. The procedure for enabling compression for the 4 Gbps Router, Extension Switch and Blade is different than the procedure for enabling compression for the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade.

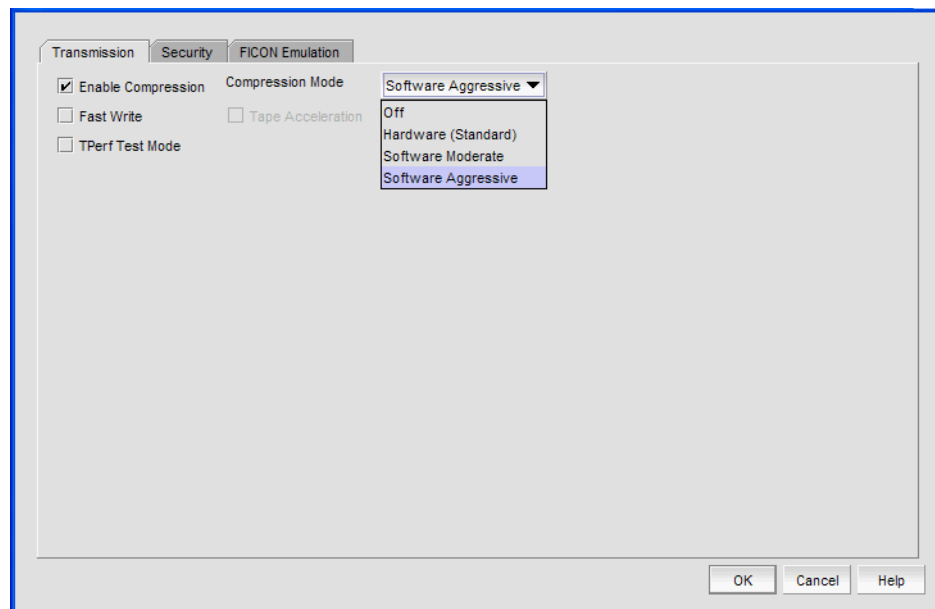
For 4 Gbps Router, Extension Switch and Blade:

1. From the **Transmission** tab, select the **Enable Compression** check box to enable compression.
2. Click **OK** to commit your selection.

For the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade:

1. Select the **Enable Compression** check box to enable compression.

This enables the **Compression Mode** selector ([Figure 157](#)).



**FIGURE 157** Selecting a compression mode

2. Select the desired compression mode.

A **Hardware** compression option is available on all platforms. The 8 Gbps 16-FC ports, 6-Gbps ports extension switch and the 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade provide two additional, more aggressive options for compression. The **Software Moderate** option enables a combination of hardware and software compression that provides more compression than hardware compression alone. This option supports up to 8 Gbps of FC traffic. the **Software Aggressive** option is a software only compression option that provides a more aggressive algorithm. This option supports up to 2.5 Gbps of FC traffic.

3. Click **OK** to commit your selection.

To disable compression, click the **Enable Compression** to clear the check mark, and click **OK**.

## Enabling Open Systems Tape Pipelining (OSTP)

Latency introduced by a long distance IP connection can negatively impact tape I/O performance. OSTP may be used to improve performance on SCSI write I/Os to sequential devices (such as tape drives). When OSTP is used, the extension blades or switches emulate write commands and responses locally to reduce delays caused by latency. Both sides of an FCIP tunnel must have matching configurations for these features to work. OSTP may be configured by selecting **Advanced Settings** on the **Add FCIP Tunnel** dialog. OSTP options are available on the **Transmission** tab.

To enable OSTP, do the following:

1. From the **Transmission** tab, select the **Fast Write** check box.  
This enables the **Tape Acceleration** check box.
2. Select the **Tape Acceleration** check box.
3. Click **OK**.

## Enabling Tperf test mode

Tperf test mode should not be enabled during normal operations. It is only used for testing and troubleshooting tunnels. Refer to the *Fabric OS FCIP Administrator's Guide* for information about Tperf.

## Configuring IPsec and IKE policies

IPsec and IKE policies are configured from the **Security** tab. The screens and procedures are platform-dependent. [Figure 158](#) shows the screen for the 4 Gbps Router, Extension Switch. [Figure 158](#) shows the screen for the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade.

1. Optionally, ensure that the peer switches on either end of the connection have known WWNs. This provides an added measure of security.
2. Assign IKE and IPsec policies. For the 4 Gbps router, Extension switch and blade, you must choose from a drop-down list of policies. The 8 Gbps router, Extension switch and blade have predefined IKE and IPsec policies. These policies are enabled by selecting the **Enable IPsec** check box. Matching policies are applied to the remote switch. Note that the **Enable IPsec** check box is grayed while editing the tunnels because the IPsec settings cannot be edited for the secured tunnels.
3. In the **PreShared Key** field, specify the key for IKE authentication. For the 4 Gbps router, Extension switch and blade, the key is between 12 and 32 alphanumeric characters. The length required depends on the chosen IKE policy. For the 8Gbps router, Extension switch and blade, the key must be 32 alphanumeric characters.

**FIGURE 158** Advanced Settings Security tab for the 4 Gbps Router, Extension Switch and Blade

These policies are used to make the connection more secure through authentication and encryption. When you select a policy for the local switch, a matching policy is automatically selected on the remote switch. If no matching policy is found, you must manually configure the policy on the remote switch.

**FIGURE 159** Advanced Settings Security Tab for the 8 Gbps extension switch and blade

#### NOTE

IPSec settings cannot be edited. If you want to change settings, you will need to delete the tunnel and then create a new tunnel with the new settings.

## Configuring FICON emulation

FICON emulation and acceleration features and operating parameters are configured from the **FICON Emulation** tab (Figure 160). Before you configure these features you must decide which features you want to implement, and you must look closely at the operational parameters to determine if values other than the default values are better for your installation.

**FIGURE 160** FICON Emulation configuration tab

1. Select the check boxes for the FICON emulation features you want to implement.

---

### NOTE

The primary FICON emulation features are XRC emulation, tape write pipelining, and tape read pipelining. TIN/TUR emulation and device level ACK emulation provide support for the three primary features. If you select any of the primary features, you must also select TIN/TUR emulation and device level ACK emulation.

---

2. Select the operational parameters for FICON emulation.
  - **FICON Tape Write Max Pipe** defines a maximum number of channel commands that may be outstanding at a given time during write pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The range is 1-100.
  - **FICON Tape Read Max Pipe** defines a maximum number of channel commands that may be outstanding at a given time during read pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The range is 1-100.
  - **FICON Tape Write Max Ops** defines a maximum number of concurrent emulated tape write operations. The range is 1-32.
  - **FICON Tape Read Max Ops** defines a maximum number of concurrent emulated tape read operations. The range is 1-32.
  - **FICON Tape Write Timer** defines a time limit for pipelined write chains. This value is specified in milliseconds (ms). If a pipelined write chain takes longer than this value to complete, the ending status for the next write chain will be withheld from the channel. This limits processing to what the network and device can support. Too small a value limits pipelining performance. Too large a value results in too much data being accepted for one device on a path. The range is 100-1500.
  - **FICON Tape Max Write Chain** defines the maximum amount of data that can be contained in a single CCW chain. If this value is exceeded, emulation is suspended. The range is 1-100.
  - **FICON Oxid Base** defines the base value of an entry pool of 256 OXIDs supplied to emulation generated exchanges. It should fall outside the range used by FICON channels and devices to avoid conflicts. The range is 0x0000 to 0xF000.
  - **FICON Debug Flags** defines optional debug flags. This is primarily for use by technical support personnel. The range is 0x00000000 to 0xFFFFFFFF.

## Viewing FCIP connection properties

The FCIP connection properties show properties of the blades or switches on both sides of a connection. To view FCIP connection properties, right-click the connection between two extension blades or switches ([Figure 161](#)).

**Product Properties**

|             | Switch1                 | Switch2                 |
|-------------|-------------------------|-------------------------|
| Domain ID   | 1                       | 5                       |
| Fabric Name | 10:00:00:05:1E:53:B6:EB | 10:00:00:05:1E:53:B6:EB |
| IP Address  | 10.32.149.203           | 10.32.149.204           |
| Name        | dcfm_sprint203          | Sprint204_name          |
| WWN         | 10:00:00:05:1E:53:C6:09 | 10:00:00:05:1E:53:B6:EB |

**Connections**

| 1-Port # | 1-Port Type | 1-WWPN                | 1-IP Address... | 1-Speed (Gb... | 2-Port # | 2-Port Type | 2-WWPN                | 2-IP Addr...  |
|----------|-------------|-----------------------|-----------------|----------------|----------|-------------|-----------------------|---------------|
| 18       | VE-Port     | 20:12:00:05:1E:53:... | 10.32.145.2     | 0              | 18       | VE-Port     | 20:12:00:05:1E:53:... | 10.32.145.12  |
| 20       | VE-Port     | 20:14:00:05:1E:53:... | 10.32.145.3     | 0              | 20       | VE-Port     | 20:14:00:05:1E:53:... | 10.32.145.13  |
| 19       | VE-Port     | 20:13:00:05:1E:53:... | 10.32.145.4     | 0              | 19       | VE-Port     | 20:13:00:05:1E:53:... | 10.32.145.14  |
| 21       | VE-Port     | 20:15:00:05:1E:53:... | 10.32.145.5     | 0              | 21       | VE-Port     | 20:15:00:05:1E:53:... | 10.32.145.15  |
| 23       | U-Port      | 20:17:00:05:1E:53:... | 10.32.149.203   | 0              | 23       | U-Port      | 20:17:00:05:1E:53:... | 10.32.149.204 |
| 22       | U-Port      | 20:16:00:05:1E:53:... | 10.32.149.203   | 0              | 22       | U-Port      | 20:16:00:05:1E:53:... | 10.32.149.204 |

**Selected Connection Properties**

|                  | Switch1 | Switch2 |
|------------------|---------|---------|
| Slot #           |         |         |
| FC Port #        | 18      | 18      |
| Port Type        | VE-Port | VE-Port |
| RA TOV           |         |         |
| ED TOV           |         |         |
| PID Format       |         |         |
| Trunking Enabled | No      | No      |
| Speed(Gbps)      | 0       | 0       |
| Tunnel ID        | 2       | 2       |
| Circuits         | 1       | 1       |

Close Help

**FIGURE 161** FCIP connection properties

# Viewing General FCIP properties

Take the following steps to view general FCIP properties.

- 1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
- 2. Select the **Properties** tab (Figure 162).

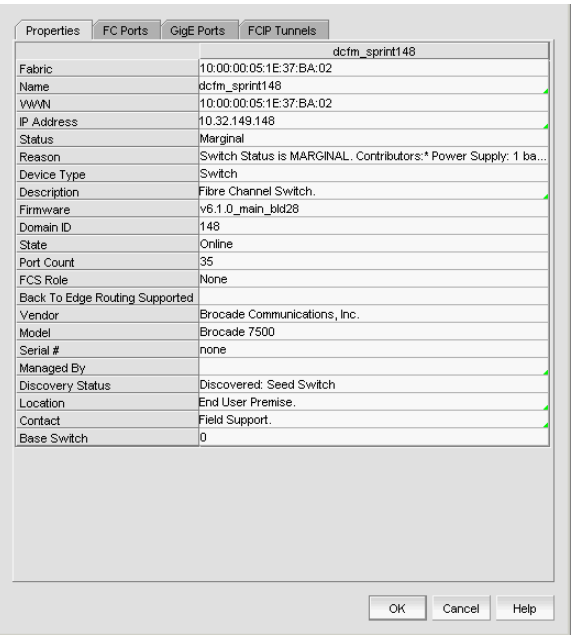


FIGURE 162 General FCIP properties tab

## Viewing FCIP FC port properties

Take the following steps to view FCIP FC port properties.

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **FC Ports** tab (Figure 163).

|                                | 0/0                     | 0/1                     |
|--------------------------------|-------------------------|-------------------------|
| Fabric                         | 10:00:00:05:1E:55:66:45 | 10:00:00:05:1E:55:66:45 |
| Switch                         | spike63                 | spike63                 |
| Name                           |                         |                         |
| Slot #                         | 0                       | 0                       |
| Port #                         | 0                       | 1                       |
| User Port #                    | 0                       | 1                       |
| Area ID (Hex)/Port Index (Hex) | 0/ 0                    | 1/ 1                    |
| FC Address                     | 630000                  | 630100                  |
| Status                         | No_Light                | Online                  |
| Additional Port Info           |                         |                         |
| State                          | Offline                 | Online                  |
| Type                           | U-Port                  | F-Port                  |
| Port Speed (Gb/s)              | 4                       | 2                       |
| Port Module                    | sw                      | lw                      |
| Port WWN                       | 20:00:00:05:1E:55:6A:45 | 20:01:00:05:1E:55:6A:45 |
| Protocol                       | FC                      | FC                      |
| Buffers Desired                | 0                       | 0                       |
| Buffers Allocated              | 0                       | 8                       |
| Distance Actual (km)           | 0                       | 0                       |
| Distance Estimated (km)        | 0                       | 0                       |
| Long Distance Setting          | L0:Normal               | L0:Normal               |
| Physical/Logical               | Physical                | Physical                |
| Locked Port Type               | U-port                  | U-port                  |
| NPIV Enabled                   | Yes                     | Yes                     |
| Connected Switch               | N/A                     | N/A                     |
| Blocked                        | No                      | No                      |
| Prohibited                     | Not Prohibited          | Not Prohibited          |

Performance

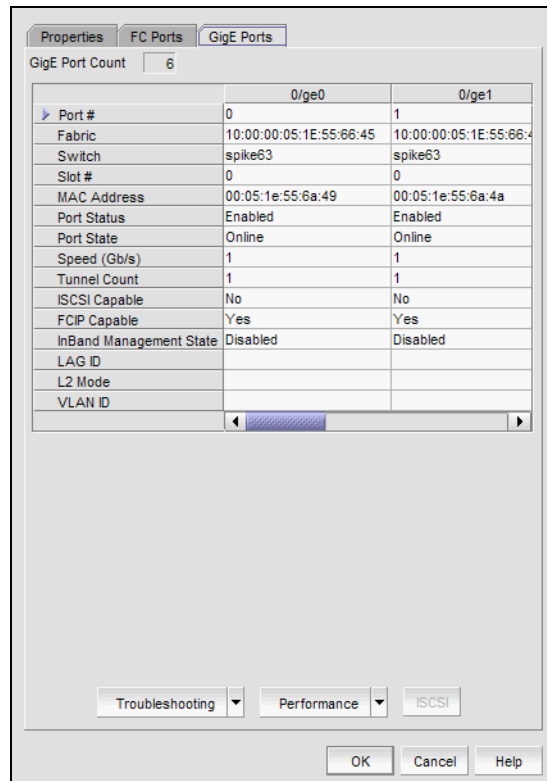
OK Cancel Help

**FIGURE 163** FC ports tab

## Viewing FCIP Ethernet port properties

Take the following steps to view Ethernet port properties.

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **GigE Ports** tab (Figure 164).



**FIGURE 164** GigE ports tab

## Editing FCIP tunnels

### NOTE

You cannot edit an active tunnel; disable the tunnel before making changes.

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to edit.
2. Select **Edit Tunnel**.

The **Edit FCIP Tunnel** dialog box displays (Figure 165).

Modify any of the settings for the tunnel and click OK.

**Switch One Settings**

Switch: MMA-12-66-FCIP

Fabric: FCIP Fabric 2

Tunnel: 20

Description: Tunnel 20.1

Port Type: ☒ VE Port ☐ VEX Port

Fabric ID:

Interop Mode: Brocade

**Switch Two Settings**

Select Switch Two

Switch: MMA-12-67-FCIP-SW

Fabric: FCIP Fabric 2

Tunnel: 20

Description: Tunnel 20.2

Port Type: ☒ VE Port ☐ VEX Port

Fabric ID:

Interop Mode: Brocade

Advanced Settings

OK Cancel Help

**FIGURE 165** Edit FCIP Tunnel dialog box

3. Fields and parameters are as described in “Configuring an FCIP tunnel”. You can edit all editable fields and parameters.

## Editing FCIP circuits

FCIP circuit settings may be edited from the **Edit FCIP Circuit** dialog box. The procedure for launching this dialog box for the 4 Gbps Router, Extension Switch and Blade is different than the procedure for the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and the 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade. The 4 Gbps Router, Extension Switch and Blade have only one circuit per tunnel, and the circuit is edited as part of the tunnel. The 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade may have multiple circuits per tunnel, and circuits may be selected individually.

For the 4 Gbps Router, Extension Switch and Blade:

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to edit.
2. Select **Edit Tunnel**.

The **Edit FCIP Tunnel** dialog box displays.

3. Select **Edit FCIP Circuit**.

The **Edit FCIP Circuit** dialog box displays.

For the 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch and the 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension blade:

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to edit.
2. Select the **Circuit** tab.
3. Select a circuit from the circuit properties table.
4. Select **Edit Circuit**.

The **Edit FCIP Circuit** dialog box displays ([Figure 166](#)).

Physical connection between the two tunnel switches is required for suggesting MTU size, maximum bandwidth and verifying IP Connectivity.

Circuit Number

| Switch One Settings                                                                                           | Switch Two Settings                                                               |
|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Switch: spike63                                                                                               | Switch: spike64                                                                   |
| Fabric: 10:00:00:05:1E:55:66:45                                                                               | Fabric: 10:00:00:05:1E:55:66:45                                                   |
| Tunnel: 16                                                                                                    | Tunnel: 16                                                                        |
| GigE Port: ge2                                                                                                | GigE Port: ge2                                                                    |
| IP Address Type: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6                             | IP Address Type: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| IP Address: 192.168.2.63                                                                                      | IP Address: 192.168.2.64                                                          |
| Subnet Mask: 255.255.255.0                                                                                    | Subnet Mask: 255.255.255.0                                                        |
| Default route will get created using the above IP address.                                                    |                                                                                   |
| <input type="checkbox"/> Create Non-Default Route                                                             |                                                                                   |
| Gateway: <input type="text"/>                                                                                 | Gateway: <input type="text"/>                                                     |
| MTU Size: 1500 (1260 - 1500) <input type="button" value="Suggest"/>                                           | MTU Size: Same as Switch One                                                      |
| Metric: 0                                                                                                     | Metric: Same as Switch One                                                        |
| VLAN ID: <input type="text"/>                                                                                 | VLAN ID: Same as Switch One                                                       |
| (Blank or 1 - 4094, Fabric OS Version >= 6.0.0)                                                               |                                                                                   |
| Bandwidth (Mb/s): <input type="radio"/> Uncommitted <input checked="" type="radio"/> Committed (10-1000 Mb/s) |                                                                                   |
| Minimum: 200.0 Maximum: 1000.0                                                                                |                                                                                   |
| <input type="button" value="Current Maximum Bandwidth"/>                                                      |                                                                                   |
| (Requires Physical Connection)                                                                                |                                                                                   |
| <input type="button" value="Verify IP Connectivity"/> <input type="button" value="Advanced Settings"/>        |                                                                                   |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>   |                                                                                   |

**FIGURE 166** Edit FCIP Circuits dialog box

- Fields and parameters are as described in [“Adding an FCIP circuit”](#). You can edit all editable fields and parameters.

## Disabling FCIP tunnels

- From the **FCIP Tunnels** dialog box, select the tunnel you want to disable.
- Select **Disable Tunnel**.

A confirmation dialog box displays, warning you that when you delete a tunnel, you delete all associated FCIP circuits.

- Click **OK** to disable the tunnel.

## Enabling FCIP tunnels

- From the **FCIP Tunnels** dialog box, select the tunnel you want to enable.
- Select **Enable Tunnel**.

A confirmation dialog box displays.

- Click **OK** to enable the tunnel.

### Deleting FCIP tunnels

1. From the **FCIP Tunnels** dialog box, right-click the tunnel you want to delete.
2. Select the **Delete Tunnel** button.  
A confirmation dialog box displays, warning you of the consequences of deleting a tunnel.
3. Click **OK** to delete the tunnel.

### Disabling FCIP circuits

1. From the **FCIP Tunnels** dialog box, right-click the tunnel that contains the circuit.
2. Select the **Circuit** tab.
3. Select the circuit from the circuit properties table.
4. Select **Disable Circuit**.  
A confirmation dialog box displays.
5. Click **OK** to disable the circuit.

### Enabling FCIP circuits

1. From the **FCIP Tunnels** dialog box, right-click the tunnel that contains the circuit.
2. Select the **Circuit** tab.
3. Select the circuit from the circuit properties table.
4. Select **Enable Circuit**.  
A confirmation dialog box displays.
5. Click **OK** to enable the circuit.

### Deleting FCIP Circuits

1. From the **FCIP Tunnels** dialog box, right-click the tunnel that contains the circuit.
2. Select the **Circuit** tab.
3. Select the circuit from the circuit properties table.
4. Select **Delete Circuit**.  
A confirmation dialog box displays, warning you of the consequences of deleting a circuit.
5. Click **OK** to delete the circuit.

## Displaying FCIP performance graphs

You can display performance graphs by clicking the **Performance** button on the FCIP Tunnels dialog box. You can also display performance graphs from Properties, as described in the following sections.

### Displaying performance graphs for FC ports

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **FC Ports** tab.
3. Click **Performance > Real Time Graph**.

### Displaying FCIP performance graphs for Ethernet ports

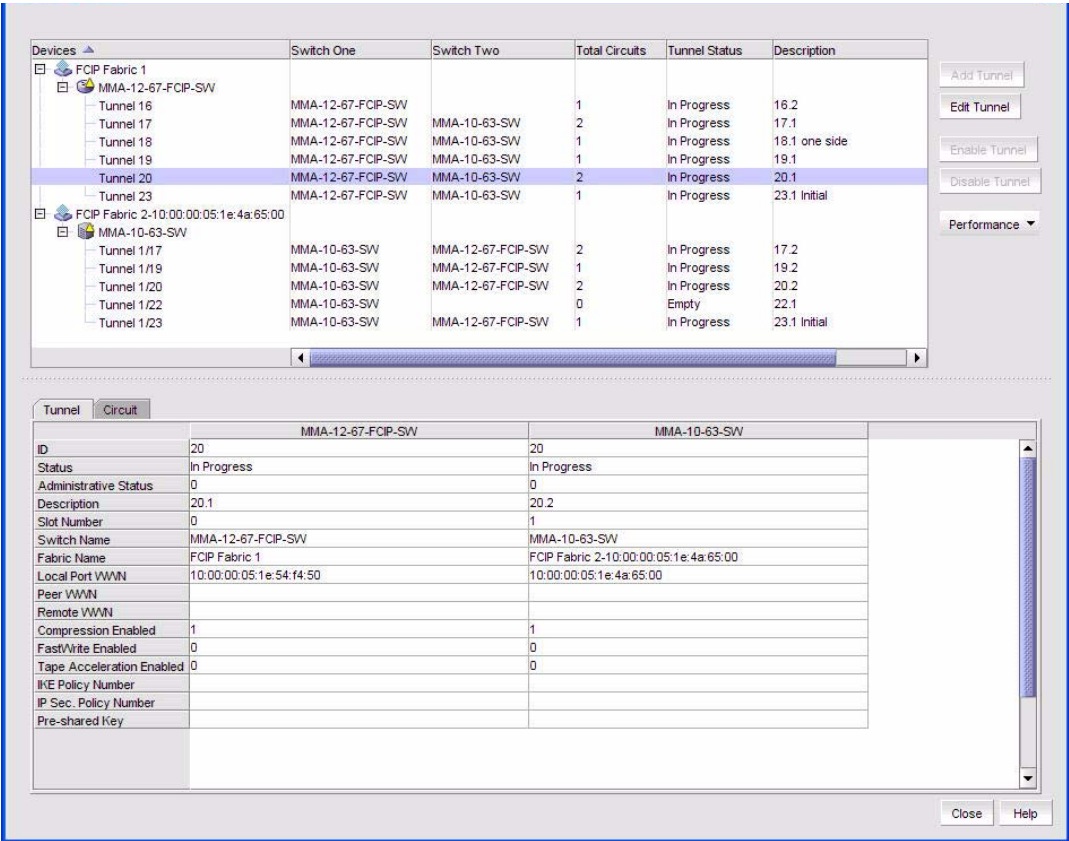
1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **GigE Ports** tab.
3. Click **Performance > Real Time Graph**.

## Displaying tunnel properties from the FCIP tunnels dialog box

Tunnel properties can be displayed from the **FCIP Tunnels** dialog box.

1. Select a tunnel from the **FCIP tunnels** dialog box.
2. Select the **Tunnel** tab.

Tunnel properties are displayed (Figure 167).



**FIGURE 167** Tunnel properties on the FCIP Tunnels dialog box

## Displaying FCIP circuit properties from the FCIP tunnels dialog box

Tunnel properties can be displayed from the **FCIP Tunnels** dialog box using the following procedure.

1. Select a tunnel from the **FCIP tunnels** dialog box.
2. Select the **Circuit** tab.

Circuit properties are displayed (Figure 168).

| Products       | Switch One | Switch Two | Total Circuits | Tunnel Operational Status | Administrative Status | Description |
|----------------|------------|------------|----------------|---------------------------|-----------------------|-------------|
| spike63        |            |            |                |                           |                       |             |
| Tunnel 16 (VE) | spike63    | spike64    | 2              | Up                        | Enabled               |             |
| Tunnel 23 (VE) | spike63    | spike64    | 4              | Up                        | Enabled               |             |
| spike64        |            |            |                |                           |                       |             |
| Tunnel 16 (VE) | spike64    | spike63    | 2              | Up                        | Enabled               |             |
| Tunnel 23 (VE) | spike64    | spike63    | 4              | Up                        | Enabled               |             |

|                                  | Circuit 0<br>spike63 | Circuit 0<br>spike64 | Circuit 1<br>spike63 | Circuit 1<br>spike64 |
|----------------------------------|----------------------|----------------------|----------------------|----------------------|
| Circuit Number                   | 0                    | 0                    | 1                    | 1                    |
| Tunnel ID                        | 16                   | 16                   | 16                   | 16                   |
| Administrative Status            | Enabled              | Enabled              | Enabled              | Enabled              |
| Operational Status               | Up                   | Up                   | Up                   | Up                   |
| GigE Port                        | ge2                  | ge2                  | ge3                  | ge3                  |
| Source IP Address                | 192.168.2.63         | 192.168.2.64         | 192.168.3.63         | 192.168.3.64         |
| Destination IP Address           | 192.168.2.64         | 192.168.2.63         | 192.168.3.64         | 192.168.3.63         |
| Gateway                          | 0.0.0.0              | 0.0.0.0              | 0.0.0.0              | 0.0.0.0              |
| MTU Size                         | 1500                 | 1500                 | 1500                 | 1500                 |
| VLAN ID                          | Not Configured       | Not Configured       | Not Configured       | Not Configured       |
| Minimum Bandwidth (Mb/s)         | 200.0                | 200.0                | 200.0                | 200.0                |
| Maximum Bandwidth (Mb/s)         | 1000.0               | 1000.0               | 1000.0               | 1000.0               |
| Selective Ack                    | On                   | On                   | On                   | On                   |
| Metric                           | 0                    | 0                    | 0                    | 0                    |
| Keep Alive Timeout (ms)          | 900                  | 900                  | 1000                 | 1000                 |
| Minimum Retransmission Time (ms) | 100                  | 100                  | 100                  | 100                  |

**FIGURE 168** Circuit properties on the FCIP Tunnels dialog box

# Displaying switch properties from the FCIP Tunnels dialog box

Switch properties are displayed on the **FCIP Tunnels** dialog box when you select a switch (Figure 169).

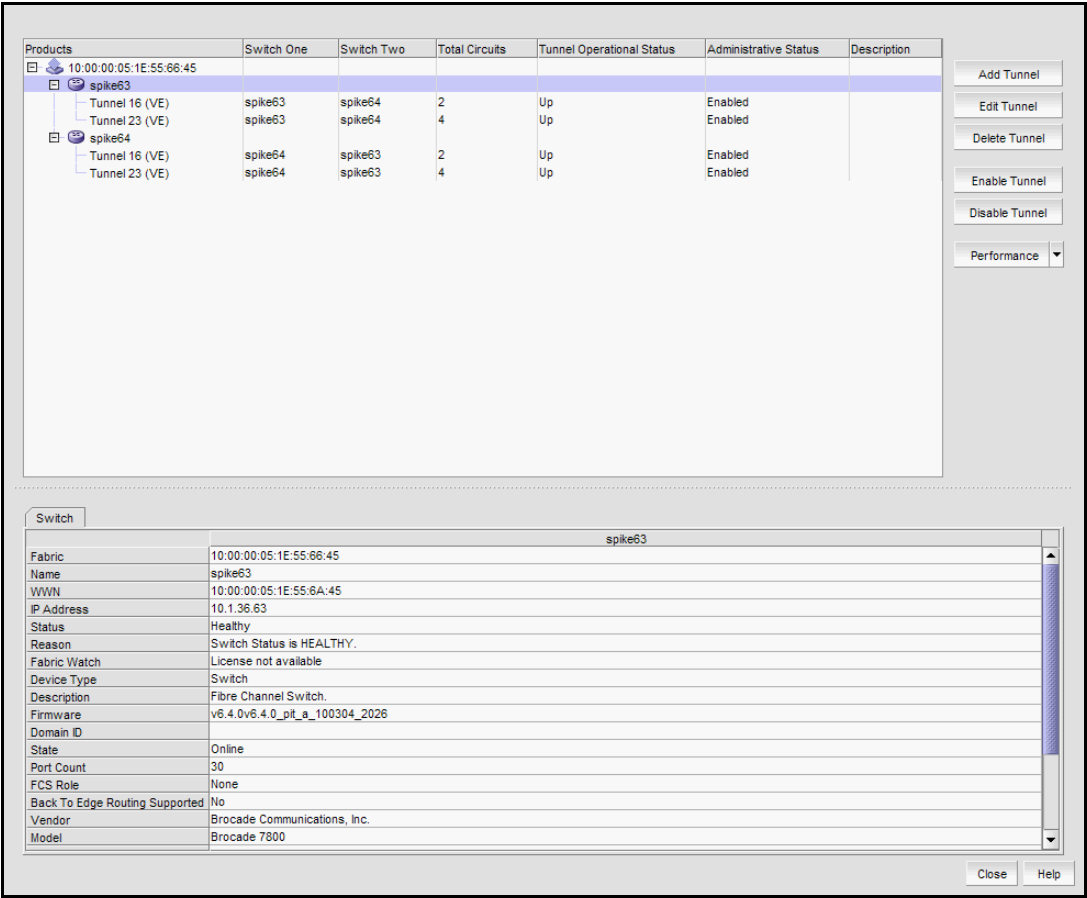


FIGURE 169    Switch properties on the FCIP Tunnels dialog box

# Displaying fabric properties from the FCIP Tunnels dialog box

Fabric properties are displayed on the FCIP Tunnels dialog box when you select a fabric.  
(Figure 170).

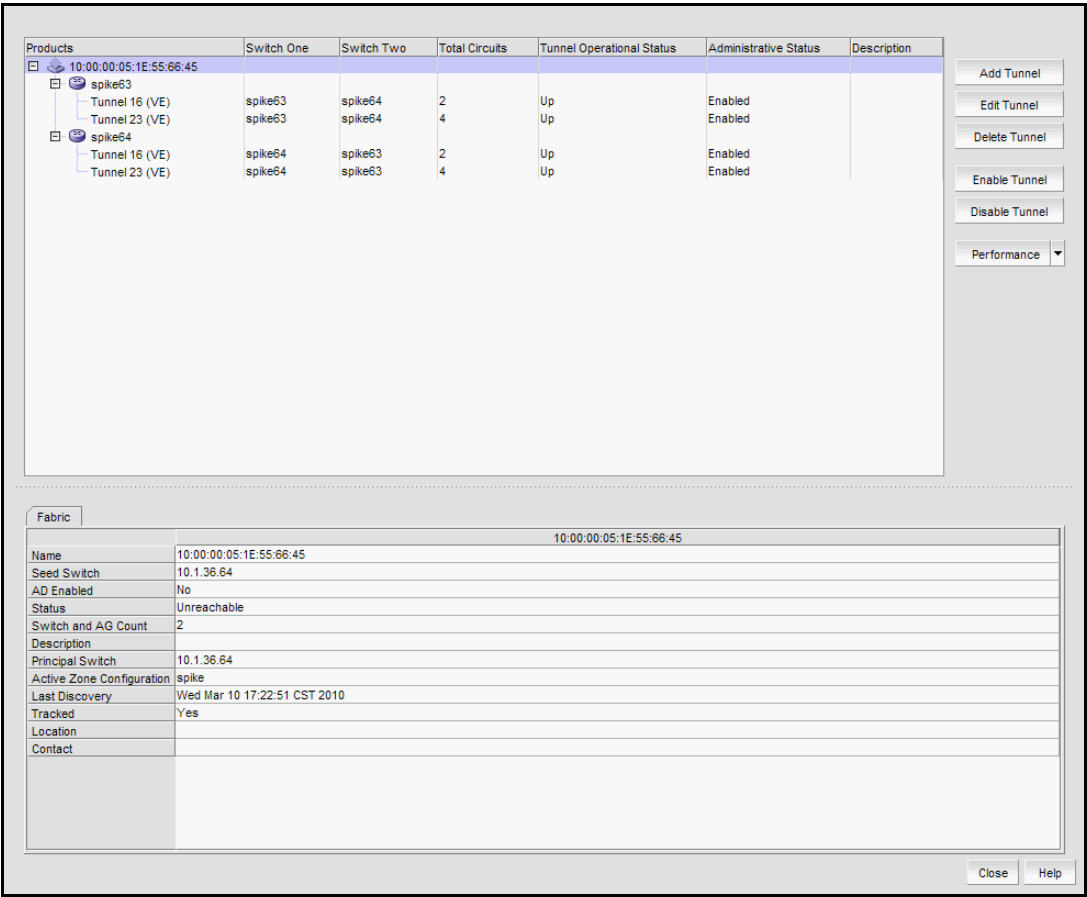


FIGURE 170 Fabric properties on the FCIP Tunnels dialog box

### Troubleshooting FCIP Ethernet connections

1. Select an extension blade or switch from the Fabric Tree structure, or right-click an extension blade or switch on the Connectivity Map, and select **Properties**.
2. Select the **GigE Ports** tab.
3. Select the Ethernet port.
4. Click **Troubleshooting**.

The following options are presented:

- **IP Ping**—Tests connections between a local Ethernet port (ge0 or ge1) and a destination IP address.
- **IP Traceroute**—Traces routes from a local Ethernet port (ge0 or ge1) to a destination IP address.
- **IP Performance**—Measures end-to-end IP path performance between a pair of FCIP ports.

# Fibre Channel over Ethernet

---

## In this chapter

- FCoE overview ..... 415
- QoS configuration ..... 437
- LLDP-DCBX configuration ..... 445
- Access Control List configuration ..... 450
- Spanning Tree Protocol configuration ..... 455
- 802.1x authentication ..... 460
- Virtual FCoE port configuration ..... 464

## FCoE overview

Fibre Channel over Ethernet (FCoE) leverages Ethernet enhancements, called *Converged Enhanced Ethernet (CEE)*, to transport encapsulated Fibre Channel frames over Ethernet. Ethernet is the physical layer over which the encapsulated FC frames are transported.

One of the barriers to using Ethernet as the basis for a converged network has been the limited bandwidth that Ethernet has historically provided. However, with 10 Gbps Ethernet, the available bandwidth now offers the potential to consolidate all the traffic types over the same link.

Unlike Fibre Channel, Ethernet is not a peer-to-peer protocol. The mechanism used to discover new ports, MAC address assignments and FC logins and logouts is called the FCoE Initialization Protocol (FIP).

## DCB exchange protocol

DCB Exchange (DCBX) protocol allows enhanced Ethernet devices to convey and configure their CEE capabilities and ensures a consistent configuration across the network. DCBX protocol is used between data center bridging (DCB) devices, such as a converged network adapter (CNA) and a FCoE switch, to exchange configuration with directly-connected peers.

---

### NOTE

When DCBX protocol is used, any other LLDP implementation must be disabled on the host systems.

---

## Enhanced Ethernet features

Converged Enhanced Ethernet (CEE) is a set of IEEE 802 standard Ethernet enhancements that enable Fibre Channel convergence with Ethernet. The two basic requirements in a lossless Ethernet environment are Enhanced Transmission Selection (ETS) and priority-based flow control. These capabilities allow the Fibre Channel frames to run directly over 10 Gbps Ethernet segments without adversely affecting performance.

### Enhanced transmission selection

Enhanced transmission selection (ETS) allows lower priority traffic classes to use available bandwidth that is not be used by higher priority traffic classes and maximizes the use of available bandwidth.

ETS allows configuration of bandwidth per priority group.

Priority group ID usage is defined as follows:

- PGID = {0, 7} is used when the priority group is limited for its bandwidth use.
- PGID = {8, 14} is reserved.
- PGID = {15} is used for priorities that are not limited for their bandwidth use.

The configured priority group percentage refers to the maximum percentage of available link bandwidth after PGID 15 is serviced, assuming all priority groups are fully subscribed. If one of the priority groups does not consume its allocated bandwidth, then any unused portion is available for use by other priority groups.

### Priority-based flow control

Priority-based flow control allows the network to selectively pause different classes of traffic and create lossless lanes for Fibre Channel, while retaining packet drop congestion management for IP traffic. A high-level pause example follows:

- During periods of heavy congestion, the receive buffers reach high threshold and generate a pause.
- The pause tells transmission (Tx) queues to stop transmitting.
- After the receive (Rx) buffers reach low threshold, a zero pause is generated.
- The zero pause signals the Tx queues to resume transmitting.

### Ethernet jumbo frames

The basic assumption underlying FCoE is that TCP/IP is not required in a local data center network and the necessary functions can be provided with Enhanced Ethernet. The purpose of an “enhanced” Ethernet is to provide reliable, lossless transport for the encapsulated Fibre Channel traffic. Enhanced Ethernet provides support for jumbo Ethernet frames and in-order frame delivery.

The Brocade FCoE 10 Gbps converged network adapter supports jumbo packets of up to 9 KB, compared to the original 1,518-byte MTU for Ethernet. The frame size increase allows the same amount of data to be transferred with less effort.

## FCoE protocols supported

The Brocade FCoE converged network adapter supports two layers of protocols: Ethernet link layer and FCoE layer. They are listed in the following sections.

### Ethernet link layer protocols supported

The following protocols support the Ethernet link layer.

- 802.1q (VLAN)
- 802.1Qaz (enhanced transmission selection)
- 802.1Qbb (priority flow control)
- 802.3ad (link aggregation)
- 802.3ae (10 Gb Ethernet)
- 802.1p (priority encoding)
- IEEE 1149.1 (JTAG) for manufacturing debug and diagnostics
- IPv4 specification (RFC 793/768)
- IPv6 specification (RFC 2460)
- TCP/UDP specification (RFC 793/768)
- ARP specification (RFC 826)
- RSS with support for IPV4TCP, IPV4, IPV6TCP, IPV6 hash types
- HDS (Header-data split)

### FCoE protocols

The following protocols support Fibre Channel over Ethernet.

- FIP (FC-BB5 compliant):
  - Support for FIP Discovery protocol for dynamic FCF discovery and FCoE link management
  - Support for FPMA and SPMA type FIP fabric login
- Support for Initiator mode only (FCP-3 compliant in Initiator mode)
- SCSI protection information support
- IP-over-FC
- NPIV support

## FCoE Licensing

The FCoE license enables Fibre Channel over Ethernet (FCoE) functionality on the Brocade 8000. Without the FCoE license, the Brocade 8000 is a pure L2 Ethernet switch and will not allow FCoE bridging capabilities.

With the FCoE license, the FCoE Configuration dialog displays virtual FCoE port information and enables you to manage the virtual port information. The topology displays directly-connected converged network adapters (CNAs) and the **Properties** dialog for the virtual FCoE port details.

Without the FCoE license, the virtual FCoE port displays in the device tree, but you cannot enable, disable, or view virtual FCoE port information.

## Save running to startup

The **Save running to startup** dialog box lists discovered CEE switches with Fabric OS version 6.3x firmware or higher. You can select available switches and move them to the Selected Switches table. Upon startup, the CEE switch configuration is copied to the selected switches.

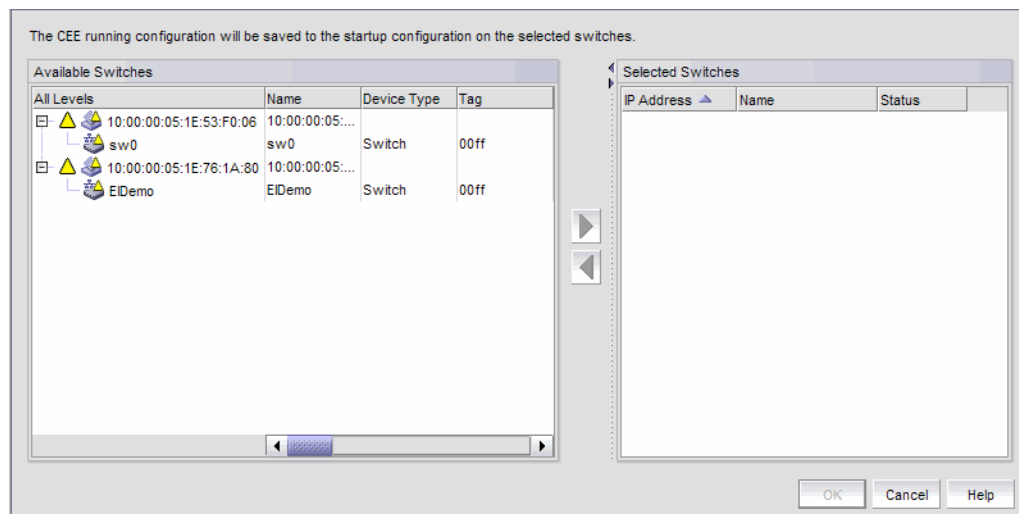
### NOTE

This dialog box launches if there is at least one CEE switch discovered. If no CEE switches exist, a warning dialog displays.

## Copying switch configurations to selected switches

1. To access the **Save running to startup** dialog box, select **Configure > Switch > Save Running to Startup** from the menu bar.

The **Save Running to Startup** dialog box displays.



**FIGURE 171** Save running to startup dialog box

2. Highlight a discovered CEE switch from the **Available Switches** table, and click the right arrow button to move the switch to the **Selected Switches** Table.
3. Highlight the selected switch and click **OK** to start the configuration.

The running configuration is saved to the selected switch, effective on the next system startup. If you restore the CEE switch using the **Restore Switch Configuration** dialog box, you are prompted to select one of two restoration methods:

- As the running configuration and reboot

---

#### **ATTENTION**

Rebooting a switch connected to a fabric will stop all traffic to and from the switch. All ports on the switch will become inactive until the switch comes back online.

---

- As the startup configuration (no reboot)

For instructions on how to restore a saved switch configuration, refer to [“Restoring a switch configuration for a selected device”](#) on page 185.

## CEE configuration

The Brocade CEE switch has 8 8-Gbps FC ports and 24 10 Gbps Ethernet CEE ports. You must configure CEE interfaces and ports differently than you configure FC ports, in order to effectively use the converged network features.

For example, Priority-based flow control (PFC) and Enhanced transmission selection (ETS) are the two QoS policy enhancements you must configure to create a lossless Ethernet. You then use DCBX protocol on CEE-enabled devices to exchange configuration information.

The CEE/FC switch module for the IBM Blade Center has 8 8-Gbps FC ports and 22/20 10 Gbps Ethernet CEE ports. The CEE ports are categorized into two types:

- External ports - the eight external ports are the same as the original 10 Gbps Ethernet CEE ports. The default name in the device tree is ExT<slot>/<port>.
- Internal ports - The default name for the 12 or 14 internal ports is InT <slot>/<port>. 802.1x, LAG configuration, and spanning tree protocol (STP) are not supported on internal ports.

Switch, CEE port, and link aggregation group (LAG) policies are discussed later in this chapter.

## Opening the CEE Configuration dialog box

1. Launch the CEE Configuration dialog box using one of the following methods:

- Select **Configure > Switch > CEE** from the menu bar.
- Right-click the CEE switch from the device tree, and select **Configure > CEE**.
- Right-click the CEE switch from the topology map and select **Configure > CEE**.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

### NOTE

The **Protocol Down Reason** column displays only if the 10 Gbps CEE/FC switch module is selected.

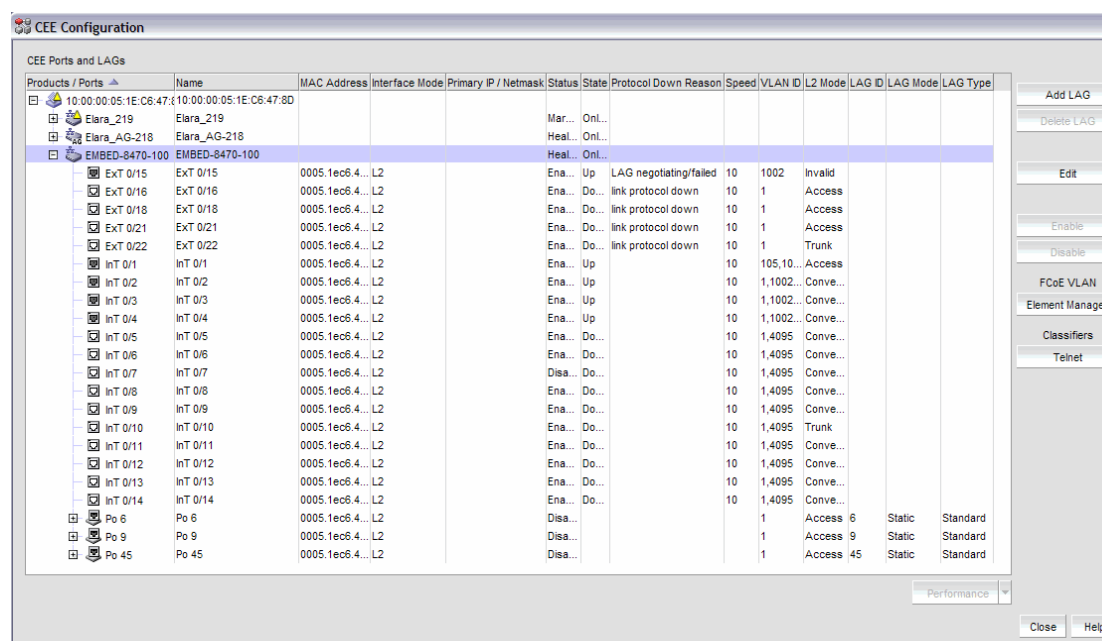


FIGURE 172 CEE configuration dialog box

2. Select the CEE switch, link aggregation group, or CEE port to perform one of the following converged enhanced Ethernet tasks, which are detailed later in this chapter.

- [“Adding a LAG” on page 427](#)
- [“Deleting a LAG” on page 434](#)
- [“Editing a LAG” on page 432](#)
- [“Enabling a CEE port or LAG” on page 434](#)

## CEE configuration tasks

The **CEE Configuration** dialog box enables you to perform the following tasks:

- Edit CEE ports for a selected switch. You can also add a link aggregation group (LAG) if a single switch is selected.
- Edit a switch or port and configure the following CEE policies:

---

**NOTE**

Access Control List and Spanning Tree Protocol can also be set at the LAG level.

---

- QoS
  - LLDP-DCBX
  - Access Control List
  - Spanning Tree Protocol
  - 802.1x
- Enable or disable a LAG or CEE port.
  - Display performance statistics for CEE ports.

Instructions for performing the CEE configuration tasks shown in [Figure 172](#) are detailed in the following sections:

- [“Link aggregation groups”](#) on page 427
- [“QoS configuration”](#) on page 437
- [“LLDP-DCBX configuration”](#) on page 445
- [“Access Control List configuration”](#) on page 450
- [“Spanning Tree Protocol configuration”](#) on page 455
- [“802.1x authentication”](#) on page 460

## Minimum CEE configuration for FCoE traffic

You must complete the following procedures to create the basic configuration of CEE for FCoE traffic.

### NOTE

The first two procedures in this section can be completed as a single procedure. They were broken into two separate procedures for clarity.

### *Creating a CEE map to carry the LAN and SAN traffic*

To create a CEE map to carry the LAN and SAN traffic, complete the following steps.

1. Select **Configure > Switch > CEE**.

The **CEE Configuration** dialog box displays.

2. Select the switch to edit in the **CEE Ports and LAGs** table and click **Edit**.

The **CEE Edit Switch** dialog box displays.

3. Click the **QoS** tab.

The **CEE Edit Switch - QoS tab** dialog box displays

Map Type: CEE

Create CEE Maps that are assignable to ports and LAGs on this switch.

CEE Map

Name: default

Precedence: 1 (1 - 100)

| PG ID | %Bandwidth | Priority Flow                               | CoS           |
|-------|------------|---------------------------------------------|---------------|
| 0.0   | 0          | <input type="checkbox"/> Enabled            |               |
| 0.1   | 0          | <input type="checkbox"/> Enabled            |               |
| 0.2   | 0          | <input type="checkbox"/> Enabled            |               |
| 0.3   | 0          | <input type="checkbox"/> Enabled            |               |
| 0.4   | 0          | <input type="checkbox"/> Enabled            |               |
| 0.5   | 0          | <input type="checkbox"/> Enabled            |               |
| 0.6   | 0          | <input type="checkbox"/> Enabled            |               |
| 0.7   | 0          | <input type="checkbox"/> Enabled            |               |
| 0     | 0          | <input type="checkbox"/> Enabled            |               |
| 40    |            | <input checked="" type="checkbox"/> Enabled | 3             |
| 60    |            | <input type="checkbox"/> Enabled            | 0,1,2,4,5,6,7 |
| 0     |            | <input type="checkbox"/> Enabled            |               |
| 0     |            | <input type="checkbox"/> Enabled            |               |
| 0     |            | <input type="checkbox"/> Enabled            |               |
| 0     |            | <input type="checkbox"/> Enabled            |               |
| 0     |            | <input type="checkbox"/> Enabled            |               |
| 0     |            | <input type="checkbox"/> Enabled            |               |

CEE Maps

| Name    | Precedence |
|---------|------------|
| default | 1          |

Duplicate Delete

Details of Selected CEE Map

| PG ID | %Bandwidth | Priority Flow | CoS |
|-------|------------|---------------|-----|
| 15.0  | 0          | Disabled      |     |
| 15.1  | 0          | Disabled      |     |
| 15.2  | 0          | Disabled      |     |
| 15.3  | 0          | Disabled      |     |
| 15.4  | 0          | Disabled      |     |
| 15.5  | 0          | Disabled      |     |
| 15.6  | 0          | Disabled      |     |
| 15.7  | 0          | Disabled      |     |

OK Cancel Help

**FIGURE 173** CEE Edit Switch dialog box - QoS tab

4. Use [“Creating a CEE map”](#) on page 438 to create a new CEE Map to carry the traffic types, as shown in the dialog box above.
5. Click **Close** on the **CEE Configuration** dialog box.

## Configuring LLDP for FCoE

To configure LLDP for FCoE, complete the following steps.

1. Select **Configure > Switch > CEE**.  
The **CEE Configuration** dialog box displays.
2. Select the switch to edit in the **CEE Ports and LAGs** table and click **Edit**.  
The **CEE Edit Switch** dialog box displays.
3. Click the **LLDP-DCBX** tab.
4. The **CEE Edit Switch - LLDP-DCBX** tab dialog box displays.

Create LLDP Profiles that will be available for assignment to ports on this switch.

☒ Enable LLDP-DCBX

**LLDP Profile**

Name: <Global Configuration>

Description:

Mode: Both Transmit and Receive

Hello(sec): 30 (Blank or 4-180)

Multiplier: 4 (Blank or 1-10)

Advertise:

- ☐ Port Description
- ☐ System Capabilities
- ☐ System Name
- ☐ System Description
- ☐ Management IP Address
- ☐ Dot1
- ☐ Dot3
- ☒ DCBX
- ☒ FCoE Application
- ☒ FCoE Logical Link

**LLDP Profiles**

| Name                   | Description |
|------------------------|-------------|
| <Global Configuration> |             |

Duplicate Delete

**Details of Selected Profile**

|            |                          |
|------------|--------------------------|
| Mode       | Both Transmit and Recel. |
| Hello      | 30                       |
| Multiplier | 4                        |
| Advertise1 |                          |
| Advertise2 |                          |
| Advertise3 |                          |
| Advertise4 |                          |
| Advertise5 |                          |
| Advertise6 |                          |
| Advertise7 |                          |

OK Cancel Help

**FIGURE 174** CEE Edit Switch dialog box - LLDP-DCBX tab

5. Select the **<Global Configuration>** LLDP profile in the **LLDP Profiles** table.
6. Click the left arrow button to edit.
7. Select the **FCoE Application** and **FCoE Logical Link** check boxes in the **Advertise** table to advertise them on the network.
8. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
9. Click **Start** on the **CEE Confirmation and Status** dialog box to save the changes to the switch.
10. Click **Close** on the **CEE Configuration** dialog box.

### *Configuring the CEE interface with the CEE Map and Global LLDP profile*

To configure the CEE interface, complete the following steps.

1. Select **Configure > Switch > CEE**.  
The **CEE Configuration** dialog box displays.
2. Select the Te port connected to the CNA in the **CEE Ports and LAGs** table and click **Edit**.
3. Select the **Port** tab, if necessary, and select the **Enable** check box.
4. Select **L2** from the **Interface Mode** list.
5. Select **Converged** (for Brocade CNA) or the **Access** (for QLogic CNA) from the **L2 Mode** list.
6. Click the **QOS** tab and select the **Assign a map to Te Port Number** check box.
7. Select **CEE** from the **Map Type** list.
8. Select the CEE map you created in [“Creating a CEE map to carry the LAN and SAN traffic”](#) on page 422 from the **Available CEE Maps** list.
9. Click the **LLDP-DCBX** tab and select the **Enable LLDP-DCBX on Te Port Number** check box.
10. Select **Assign the Global Configuration**.
11. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
12. Click **Start** on the **CEE Confirmation and Status** dialog box to save the changes to the switch.
13. Click **Close** on the **CEE Configuration** dialog box.

### *Create the FCoE VLAN to carry FCoE traffic*

---

#### **NOTE**

This procedure is completed using Web Tools. For more information, see [“CEE switch management using Web Tools”](#) on page 463.

---

To create the FCoE VLAN, complete the following steps.

1. Select the Brocade FCoE switch in the Product Tree or Connectivity Map.
2. Select **Configure > Element Manager > Admin**.  
Web Tools displays. You can also launch Web Tools by clicking the **Element Manager** button on the CEE Configuration dialog box.
3. Click the **CEE** tab.
4. Click the **VLAN** tab.
5. Click **Add**.  
The **VLAN Configuration** dialog box displays.
6. Enter the VLAN identifier in the VLAN ID field.
7. Click **OK** on the **VLAN Configuration** dialog box.  
The **VLAN Configuration** dialog box displays.
8. Select the VLAN you created and click **Edit** to convert the VLAN to FCoE VLAN.

9. Select the **FCoE** check box.
10. Select the CEE interface to carry the FCoE traffic from the **Selection List** and click **Add** to add it to the **Selected List**.
11. Click **OK** on the **VLAN Configuration** dialog box to save your changes.
12. Close Web Tools.

### *Creating VLAN classifiers and activating on the CEE interface*

---

#### **NOTE**

This procedure is completed using the CLI. For more information, see [“CEE switch management using Telnet”](#) on page 464.

---

To create and activate the VLAN classifiers on the CEE interface, complete the following steps.

1. Log into the switch and enter global configuration mode.

#### **Example**

```
switch:<userid>>cmsh
switch#configure terminal
```

2. Create and apply VLAN Classifiers to the CEE interface to classify Ethernet frames on an untagged interface to VLAN.

#### **Example**

```
switch(config)#vlan classifier rule 1 proto fip encap ethv2
switch(config)#vlan classifier rule 2 proto fcoe encap ethv2
switch(config)#vlan classifier group 1 add rule 1
switch(config)#vlan classifier group 1 add rule 2
```

3. Apply the VLAN classifier Group to the CEE interface.

#### **Example of activating VLAN classifier on the interface Te 0/7**

```
switch(conf-if-te-0/7)#vlan classifier activate group 1 vlan 1002
```

4. Save the **running-config** file to the startup-config file.

#### **Example**

```
switch#copy running-config startup-config
```

## Switch policies

You can configure and enable a number of CEE policies on a switch, port, or link aggregation group (LAG).

The following switch policy configurations apply to all ports in a LAG:

- CEE map and Traffic Class map
- Link Layer Discovery Protocol (LLDP)

The following switch policy configurations apply to the LAG itself:

- Access Control Lists (ACL)
- Spanning Tree Protocol (STP)

The switch policies are described in the following sections.

### CEE map and Traffic Class map

With CEE, Fibre Channel uses a buffer management system based on buffer-to-buffer credits, with corresponding confirmation by the R-RDY frame. The flow control standard used for CEE is based on “pause” frames. Coupled with an appropriate input buffer, lossless transport of frames is possible.

Priority-based flow control (PFC) deals with the prioritization of frames. This standard IEEE 802.1Q allows application-specific bandwidth reservations in CEE. When you create a CEE map, you specify the precedence (priority) and then you map the priority groups with the Class of Service (CoS) and apply bandwidth percentages.

Refer to [“QoS configuration”](#) on page 437 for instructions on how to create CEE and Traffic Class maps.

### LLDP profiles

Data Center Bridging Capability Exchange Protocol (DCBX) enables Enhanced Ethernet devices to discover whether a peer device supports particular features, such as Priority Flow Control or Class of Service (CoS). In a Converged Enhanced Ethernet (CEE) environment, LLDP is enhanced with DCBX protocol to further share or change the configured CEE enhancements.

Refer to [“LLDP-DCBX configuration”](#) on page 445 for instructions on how to create LLDP profiles.

### Access control lists

Access control lists (ACL) are sequential lists consisting of permit and deny rules. They are either Layer 3 (IP)- or Layer 2 (MAC)-specific. You can configure multiple access lists and rules and store them in the configuration. You create an ACL on a switch and then you can apply the configuration to ports, and link aggregation groups (LAGs) on that switch.

Refer to [“Access Control List configuration”](#) on page 450 for instructions on how to create and manage access control lists.

## Spanning Tree Protocol policy

The Spanning Tree Protocol (STP) is a Layer 2 protocol that ensures a loop-free topology for any bridged LAN (Layer-2 bridges are typically Ethernet switches). Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops or the need to manually enable or disable these backup links.

---

**NOTE**

STP is not supported on internal ports.

---

Refer to [“Spanning Tree Protocol configuration”](#) on page 455 for more information.

## 802.1x policy

802.1x is a standard authentication protocol that defines a client-server-based access control and authentication protocol. 802.1x restricts unknown or unauthorized clients from connecting to a LAN through publicly accessible ports.

Refer to [“802.1x authentication”](#) on page 460 for information on setting 802.1x parameters.

## Link aggregation groups

Link aggregation, based on the IEEE 802.3ad protocol, is a mechanism to bundle several physical ports together to form a single logical channel or trunk. The collection of ports is called a link aggregation group (LAG). LAG configuration is not supported on internal ports.

The **Add LAG** button is enabled when a single CEE switch or ports of a single CEE switch are selected. The **Add LAG** button is disabled when multiple switches are selected, ports from different switches are selected, or LAGs are selected.

The **Edit button** is enabled when a single LAG, port, or switch is selected.

---

**NOTE**

When LLDP-DCBX, Access Control List (ACL), or Spanning Tree Protocol (STP) is disabled on the switch, a yellow banner displays on the dialog box, indicating that LLDP-DCBX, ACL, or STP is not only disabled on the switch, it is also disabled for all ports and LAGs on the switch.

---

## Adding a LAG

You manage port selection using the **Add LAG** dialog.

---

**NOTE**

An internal port cannot be part of a LAG. You can create LAGs with external ports only.

---

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select the CEE switch or one or more CEE ports to add to a link aggregation group (LAG).

## 3. Click **Add LAG**.

The **Add LAG** dialog box displays.

The screenshot shows the 'Add LAG' dialog box with the 'LAG' tab selected. The 'LAG ID' field is empty, with a range '(1 - 63)' indicated. 'Interface Mode' is set to 'L2'. 'Status' has an 'Enable' checkbox. 'L2 Mode' is set to 'Access'. 'Type' is 'Standard'. 'Mode' has 'Static' and 'Dynamic' radio buttons, with 'Dynamic' selected. 'IP / Netmask' has 'Primary' and 'Secondary' fields. 'Available Members' is a list of ports from Te 0/0 to Te 0/15, all checked. 'LAG Members' is a table with 'Port' and 'Dynamic Mode' columns, showing 'Te 0/1' as 'Active'. 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

**FIGURE 175** Add LAG dialog box

## 4. Configure the following LAG parameters:

### NOTE

Ports with 802.1x authentication or ports that are L2 or L3 mode-enabled are not supported in a LAG.

- **Status** - Enabled or Disabled. You must enable the LAG to use the CEE functionality.
- **LAG ID** - Enter the LAG identifier, using a value between 1-63. Duplicate LAG IDs are not allowed.
- **Interface mode** - none or L2.
  - ☐ The L3 interface mode option is displayed in the Edit LAG dialog box only.
- **L2 interface mode** - Select the L2 mode (Access or Trunk):
  - ☐ Access mode allows only one VLAN and allows only untagged frames.
  - ☐ Trunk mode allows more than one VLAN association and allows tagged frames.
  - ☐ A converged mode interface can be native (Access, untagged frames) in one VLAN and non-native (Trunk, tagged frames) in another VLAN.
- **IP/Netmask** - The netmask is used to divide an IP address into subnets. It specifies which portion of the IP address represents the network and which portion represents the host, and can only be configured if the interface mode is L3.
  - ☐ Primary - The primary IP address assigned to a 10 Gbps CEE/FC switch module.
  - ☐ Secondary - The secondary IP address is optional. Secondary IP addresses are helpful when the interface port is part of multiple subnets.

5. Select at least one available CEE port from the **Available Members** table and click the right arrow button to move them to the **LAG Members** table.

The CEE ports are now part of the link aggregation group.

6. Continue to configure the following LAG parameters. These parameters are always enabled.
  - **Mode** - Sets all ports added to the LAG members table in either Static or Dynamic mode. The default is Dynamic, Active, but LAG members can be Active or Passive if the LAG member is Dynamic.
  - **Type** - Sets the limit on the size of the LAG. The type values include Standard, where the LAG is limited to 16 ports, and Brocade, where the LAG is limited to four ports. The default is Standard.

---

**NOTE**

The 8 Gbps 16-FC-port, 10 GbE 8-Ethernet Port have three anvil chips and each anvil chip supports eight 10 Gbps Ethernet ports. You cannot create Brocade-type LAGs from different anvil chips. If you do, an error message displays and only the first port is considered as part of the LAG.

---

7. When you have finished configuring the policies, click **OK**.

The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

If the operation was successful, the new LAG displays in the custom products list in the **CEE Configuration** dialog.

## Editing a CEE switch

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select the CEE switch from the **Products/Ports** table.
3. Click **Edit**.

The **Edit Switch** dialog box displays (Figure 176).

**FIGURE 176** Edit Switch dialog box

4. Configure the policies for the Edit Switch tabs, which are described in the following sections:
  - “[QoS configuration](#)” on page 437
  - “[LLDP-DCBX configuration](#)” on page 445
  - “[Access Control List configuration](#)” on page 450
  - “[Spanning Tree Protocol configuration](#)” on page 455
  - “[802.1x authentication](#)” on page 460
5. When you have finished configuring the policies, apply the settings to the switch.

---

### NOTE

Clicking **Cancel** when there are pending changes launches a pop-up dialog.

---

6. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Editing a CEE port

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a CEE port from the Products/Ports table.
3. Click **Edit**.

The **Edit Port** dialog box displays.

**FIGURE 177** Edit Port dialog box

4. Modify the following CEE Port parameters as required:
  - **Status** - Enable or Disable. You must enable the LAG to use the CEE functionality.
  - **Interface Mode** - None or L2. For external ports, the **L3** interface mode displays, in addition to None or L2. If you select L3 as the interface mode, the IP/Netmask field is enabled and you can then assign the primary and secondary IP addresses.
    - ☐ **L2 Mode** - This is enabled if you select L2 as the Interface Mode. If a CEE port is enabled on the 10 Gbps CEE/FC switch module, the L2 mode is disabled.
    - ☐ **L3 Mode** appears only for the 10 Gbps CEE/FC switch module port.

---

### NOTE

You cannot change the Interface Mode to **None** if it is set to **L2** and the port is assigned to a VLAN.

---

- **IP/Netmask** - The netmask is used to divide an IP address into subnets. It specifies which portion of the IP address represents the network and which portion represents the host, and can only be configured if the interface mode is L3.
  - ☐ **Primary** - The primary IP address assigned to a 10 Gbps CEE/FC switch module.
  - ☐ **Secondary** - The secondary IP address is optional. Secondary IP addresses are helpful when the interface port is part of multiple subnets.

- When you have finished configuring the policies, apply the settings to the CEE port.

**NOTE**

Clicking **Cancel** when there are pending changes launches a pop-up dialog.

- Click **OK** when you have finished modifying the CEE port parameters.  
The **CEE Confirmation and Status** dialog box displays.
- Review the changes carefully before you accept them.
- Click **Start** to apply the changes, or click **Close** to abort the operation.

## Editing a LAG

Use the following procedure to change members and policies in a link aggregation group (LAG).

- Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
- Select the link aggregation group (LAG) from the **Products/Ports** table.
- Click **Edit**.

The **Edit LAG** dialog box displays.

The screenshot shows the 'Edit LAG' dialog box with the following details:

- Tabs:** LAG, QoS, LLDP-DCBX, Access Control List, Spanning Tree Protocol.
- LAG ID:** 1 (range 1 - 63)
- Interface Mode:** L2
- Status:** ☒ Enable
- L2 Mode:** Access
- Type:** Standard
- Mode:** ☐ Static, ☒ Dynamic
- IP / Netmask:** Primary and Secondary fields.
- Available Members Table:**

| Port                                        |
|---------------------------------------------|
| <input checked="" type="checkbox"/> Te 0/0  |
| <input checked="" type="checkbox"/> Te 0/2  |
| <input checked="" type="checkbox"/> Te 0/3  |
| <input checked="" type="checkbox"/> Te 0/4  |
| <input checked="" type="checkbox"/> Te 0/5  |
| <input checked="" type="checkbox"/> Te 0/6  |
| <input checked="" type="checkbox"/> Te 0/7  |
| <input checked="" type="checkbox"/> Te 0/8  |
| <input checked="" type="checkbox"/> Te 0/9  |
| <input checked="" type="checkbox"/> Te 0/10 |
| <input checked="" type="checkbox"/> Te 0/11 |
| <input checked="" type="checkbox"/> Te 0/12 |
| <input checked="" type="checkbox"/> Te 0/13 |
| <input checked="" type="checkbox"/> Te 0/14 |
| <input checked="" type="checkbox"/> Te 0/15 |
- LAG Members Table:**

| Port                                       | Dynamic Mode |
|--------------------------------------------|--------------|
| <input checked="" type="checkbox"/> Te 0/1 | Active       |
- Buttons:** OK, Cancel, Help.

**FIGURE 178** Edit LAG dialog box

- Modify the following LAG parameters as required:

5. Configure the following LAG parameters:

---

**NOTE**

Ports with 802.1x authentication or ports that are L2/L3 mode enabled are not supported in a LAG.

---

- **Status** - Enabled or Disabled. You must enable the LAG to use the CEE functionality.
- **LAG ID** - The LAG identifier, which is not an editable field.
- **Interface Mode** - L2 or none. For external ports, the **L3** interface mode displays, in addition to None or L2. If you select L3 as the interface mode, the IP/Netmask field is enabled and you can then assign the primary and secondary IP addresses.
  - A port must be in non-L2 Mode if you are adding the port as a member of a LAG.
  - You cannot change the Interface Mode from **L2** to **none** if the LAG is assigned to a VLAN.
- **L2 Mode** - Select the L2 mode (Access or Trunk).
  - ☐ Access mode allows only one VLAN and allows only untagged frames.
  - ☐ Trunk mode allows more than one VLAN association and allows tagged frames.
- **Primary** - Enter the primary IP address assigned to an L3 port.

---

**NOTE**

Primary and secondary IP fields are applicable only to the external ports and the interface mode must be L3 to enable these fields.

---

- **Secondary** - Enter the secondary IP address (optional). Multiple (secondary) IP addresses help when the interface and port are part of multiple subnets.
6. Select at least one available CEE port from the **Available Members** table and click the right arrow button to move them to the **LAG Members** table.  
The CEE ports are now part of the link aggregation group.
  7. Continue to configure the following LAG parameters. These parameters are disabled until you add a CEE port to the **LAG members** table.
    - **Mode** - The ports that are LAG members are in either Static or Dynamic mode. You cannot change the mode on existing members of a LAG.  
  
If the mode is set as Dynamic, you can change the dynamic mode type (to Active or Passive) only for newly-added ports, not for existing port members of a LAG.
    - **Type** - The type value options are **Standard**, where the LAG is limited to 16 ports, and **Brocade**, where the LAG is limited to four ports. The default is **Standard**. The type is set when you add a LAG; you cannot edit the type using the **Edit LAG** dialog box.
  8. Click **OK** when you have finished modifying the LAG parameters.  
The **CEE Confirmation and Status** dialog box displays.
  9. Review the changes carefully before you accept them.
  10. Click **Start** to apply the changes, or click **Close** to abort the operation.

---

**NOTE**

If the primary or secondary IP address already exists on another interface, an error message displays in the **Status** area.

---

## Enabling a CEE port or LAG

If you select multiple switches or multiple ports and LAGs from two or more switches, both the **Enable** button and the **Disable** button are disabled.

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select one or more CEE ports or LAGs (which can span multiple switches) that you want to enable.

---

### NOTE

All selected LAGs must be in the same state (enabled or disabled); otherwise, both the **Enable** and **Disable** buttons are disabled.

---

3. Click **Enable**.

The selected CEE port or LAG is enabled for CEE configuration.

4. Click **OK**.

The **CEE Confirmation and Status** dialog box displays.

5. Review the changes carefully before you accept them.

6. Click **Start** to apply the changes, or click **Close** to abort the operation.

The selected CEE port or LAG is enabled for CEE configuration. (The **Status** column in the **CEE Configuration** dialog reflects the change).

## Deleting a LAG

You can only delete a link aggregation group (LAG) that is selected from a single switch. If you select multiple switches or multiple ports from two or more switches, the **Delete** button is disabled.

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select one or more LAGs (that can span multiple switches) that you want to delete from the **Products/Ports** table.

3. Click **Delete**.

4. Click **OK**.

The **CEE Confirmation and Status** dialog box displays.

5. Review the changes carefully before you accept them.

6. Click **Start** to apply the changes, or click **Close** to abort the operation.

The LAG is removed from the **Products/Ports** list and any of the LAG members display without the LAG containment.

## CEE Performance

Performance monitoring provides details about the quantity of traffic and errors a specific port or device generates on the fabric over a specific time frame. You can also use performance to indicate the devices that create the most traffic and to identify the ports that are most congested.

### Real Time Performance Graph

You can monitor a device's performance through a performance graph that displays transmit and receive data. The graphs can be sorted by the column headers. You can create multiple real-time performance graph instances.

#### *Generating a real-time performance graph.*

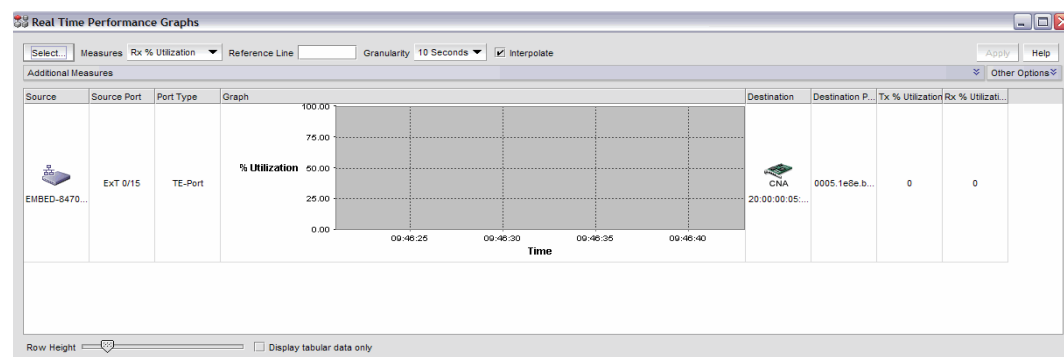
To generate a real-time performance graph for a device, complete the following steps.

1. Select a CEE port from the **CEE Configuration** dialog box, and select **Real Time Graph** from the Performance list.

A message displays, prompting you to close the **CEE Configuration** dialog box.

2. Click **OK** to close the **CEE Configuration** dialog and open the Performance dialog box.

The **Real Time Performance Graphs** dialog box displays.



**FIGURE 179** Real Time Performance Graphs dialog box

For complete information about Real Time Performance Graphs, refer to [“Real-time performance data”](#) on page 293.

## Historical Performance Graph

The **Historical Performance Graph** dialog box enables you to customize how you want the historical performance information to display.

### *Generating a historical performance graph*

1. Select a CEE port from the **CEE Configuration** dialog box, and select **Historical Graph** from the Performance list.

A message displays, prompting you to close the **CEE Configuration** dialog.

2. Click **OK** to close the **CEE Configuration** dialog and open the Performance dialog box.

The **Historical Performance Graph** dialog box displays.

For complete information about Real Time Performance Graphs, refer to [“Real-time performance data”](#) on page 293.

## Historical Performance Report

The **Historical Performance Report** dialog box enables you to customize how you want the historical performance information to display.

### *Generating a historical performance report.*

1. Select a CEE port from the **CEE Configuration** dialog box, and select **Historical Report** from the Performance list.

A message displays, prompting you to close the **CEE Configuration** dialog box.

2. Click **OK** to close the **CEE Configuration** dialog and open the Performance dialog box.

The **Historical Performance Report** dialog box displays.

PDF Export To [Navigation Icons] 75% Close

**Historical Performance Report**

Server: {4BP-2CE936TN42} @ IP Address : {172.16.66.59}

**Report Configuration**

Favorite Name: Default-Last 1Hr-Tx-Rx-%Utilization  
 Main Measure: Rx % Utilization  
 Display: Top 5 of Rx % Utilization  
 From: Selected TE Ports  
 For: Last 1 Hour  
 Granularity: 5 Minutes  
 Additional Measures:

**Top 5 of Selected TE Ports by Rx % Utilization**

| # | Fabric | Source | Source Port | Port Type | Destination | Destination Port | Rx % Utilization |
|---|--------|--------|-------------|-----------|-------------|------------------|------------------|
|---|--------|--------|-------------|-----------|-------------|------------------|------------------|

**FIGURE 180** Historical Performance Report dialog box

For complete information about Historical Performance Graphs, refer to [“Historical performance data”](#) on page 297.

## QoS configuration

QoS configuration involves configuring packet classification, mapping the priority and traffic class, controlling congestion, and scheduling. The configuration of these QoS entities consist of CEE Map and Traffic Class Map configuration.

In a Converged Enhanced Ethernet (CEE) configuration, Enhanced Transmission Selection (ETS) and Priority-based flow control (PFC) are configured by utilizing a priority table, a priority group table, and a priority traffic table. The Traffic Class Map is the mapping of user priority to traffic class.

### Enhanced Transmission Selection

Enhanced Transmission Selection (ETS) allows lower priority traffic classes to use available bandwidth not being used by higher priority traffic classes and maximizes the use of available bandwidth.

### Priority-based flow control

Priority based flow control (PFC) is an enhancement to the existing pause mechanism in Ethernet. PFC creates eight separate virtual links on the physical link and allows any of these links to be paused and restarted independently, enabling the network to create a no-drop class of service for an individual virtual link.

[Table](#) shows examples of how priority grouping might be allocated in a 15-priority group scenario.

| Priority group ID | Bandwidth (%)                        | Priority flow control |
|-------------------|--------------------------------------|-----------------------|
| 0                 | 55                                   | on                    |
| 1                 | 25                                   | on                    |
| 2                 | 0                                    | off                   |
| 3                 | 0                                    | off                   |
| 4                 | 5                                    | off                   |
| 5                 | 0                                    | off                   |
| 6                 | 15                                   | on                    |
| 7                 | 0                                    | off                   |
| 15.0-15.7         | Strict priority                      | on                    |
|                   | No bandwidth % configuration allowed |                       |

## Creating a CEE map

When you create a CEE map, each of the Class of Service (CoS) options (0-7) must be mapped to at least one of the Priority Group IDs (0-7) and the total bandwidth must equal 100. All QoS, CEE map, and Traffic map configurations apply to all ports in a LAG.

There can be, at the most, 16 entries in the Priority Group table. Eight of the entries are Strict Priority entries with a Priority Group ID of 15.0 to 15.7 and eight are user-definable entries with a Priority Group ID of 0-7. See [Table](#) for an example of priority group configuration.

## NOTE

The 10 Gbps CEE/FC switch module can have only one CEE map.

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.

- Click the **QoS** tab on the **Edit Switch** dialog box.

The **QoS** dialog box displays.

GoS LLDAP-DCBX Access Control List Spanning Tree Protocol 802.1x

Map Type CEE

Create CEE Maps that are assignable to ports and LAGs on this switch.

### CEE Map

Name

Precedence  (1 - 100)

#### Priority Group Table

| PG ID | %Bandwidth | Priority Flow                               | CoS |
|-------|------------|---------------------------------------------|-----|
| 15.0  | 0          | <input type="checkbox"/> Enabled            |     |
| 15.1  | 0          | <input type="checkbox"/> Enabled            |     |
| 15.2  | 0          | <input type="checkbox"/> Enabled            |     |
| 15.3  | 0          | <input type="checkbox"/> Enabled            |     |
| 15.4  | 0          | <input type="checkbox"/> Enabled            |     |
| 15.5  | 0          | <input type="checkbox"/> Enabled            |     |
| 15.6  | 0          | <input type="checkbox"/> Enabled            |     |
| 15.7  | 0          | <input type="checkbox"/> Enabled            |     |
| 0     |            | <input checked="" type="checkbox"/> Enabled |     |
| 1     |            | <input type="checkbox"/> Enabled            |     |
| 2     |            | <input checked="" type="checkbox"/> Enabled |     |
| 3     |            | <input type="checkbox"/> Enabled            |     |
| 4     |            | <input checked="" type="checkbox"/> Enabled |     |
| 5     |            | <input type="checkbox"/> Enabled            |     |
| 6     |            | <input checked="" type="checkbox"/> Enabled |     |
| 7     |            | <input type="checkbox"/> Enabled            |     |

### CEE Maps

| Name    | Precedence |
|---------|------------|
| default | 1          |

Delete

#### Details of Selected CEE Map

| PG ID | %Bandwidth | Priority Flow | CoS           |
|-------|------------|---------------|---------------|
| 1     | 40         | Enabled       | 3             |
| 2     | 60         | Disabled      | 0,1,2,4,5,6,7 |
| 15.0  | 0          | Disabled      |               |
| 15.1  | 0          | Disabled      |               |
| 15.2  | 0          | Disabled      |               |
| 15.3  | 0          | Disabled      |               |
| 15.4  | 0          | Disabled      |               |

OK Cancel Help

**FIGURE 181** QoS, Create CEE Map dialog box

4. Select CEE from the **Map Type** list.

5. Configure the following CEE Map parameters in the **CEE Map** table:

- **Name** - Enter a name to identify the CEE map. If the switch is a 10 Gbps CEE/FC switch module, you cannot change the name.
- **Precedence** - Enter a value between 1 - 100. This number determines the map's priority.
- **Priority Flow Control** check box - Check to enable priority flow control on individual priority groups.
- **CoS** - Enter a Class of Service value to correspond to the Priority Group ID rows. All of the eight CoS values (0-7) must be used in a CEE map. Duplicate CoS values in two or more priority groups are not allowed.

---

**NOTE**

You can only edit CoS fields that are displayed with a green tick mark.

---

**% Bandwidth** (*optional*) - Enter a bandwidth value for priority group (PG) IDs 0-7. You must map each CoS to at least one of the PG IDs. Use a comma or a space to separate multiple CoS values, as shown in [Figure 181](#).

Note the following points:

- You cannot define a bandwidth percentage for Strict Priorities (PG ID 15.0 - 15.7). The total % Bandwidth for PG ID 15.0-15.7 must equal 0%.
- If you set a CoS value to one or more of the PG IDs 0-7, you must also enter a non-0% bandwidth percentage. The total % Bandwidth must equal 100%.
- For PG IDs 0-7 that do not have an assigned CoS value or PFC enabled, the % Bandwidth must be 0%.

6. Click the right arrow button to add the map to the CEE Maps table.

If a CEE map exists with the same name, a validation dialog box launches and you are asked if you want to overwrite the map.

7. Click **OK**.

The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.

9. Click **Start** to apply the changes, or click **Close** to abort the operation. If any configuration errors exist in the CEE map, an error message displays in the **Status** area.

## Editing a CEE map

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.

3. Click the **QoS** tab on the **Edit Switch** dialog box.

The **QoS** dialog box displays.

4. Select a CEE Map from the **CEE Maps** table, and click the left arrow button to load its values to the left pane. The fields are now editable.

## 17 Deleting a CEE map

5. Keep the same CEE Map name and modify the following values, as required. See [Table](#) for an example of priority group configuration.
  - **Name** - Enter a name to identify the CEE map. If the switch is a 10 Gbps CEE/FC switch module, you cannot change the name.
  - **Precedence** - Enter a value between 1 - 100. This number determines the map's priority.
  - **% Bandwidth** - Enter a bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100%.
  - **Priority Flow Control** check box - Check to enable priority flow control on individual priority groups.
  - **CoS** - Enter a Class of Service value to correspond to the Priority Group ID rows. Each CoS must be mapped to at least one of the Priority Group IDs (0-7), separated with a comma and a space, as shown in [Figure 181](#).
6. Click the right arrow button to re-add the map to the CEE Maps table.  
If the CEE Map already exists, an overwrite message displays.
7. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation. If any configuration errors exist in the CEE map, an error message displays in the **Status** area.

### Deleting a CEE map

You cannot delete the CEE map of a 10 Gbps CEE/FC switch module.

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.  
The **QoS** dialog box displays.
4. Select a CEE Map that you want to delete from the **CEE Maps** table.
5. Click **Delete**.  
The Delete confirmation dialog displays.
6. Click **Yes** to confirm.  
The CEE Map row is removed from the table.
7. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

If a CEE map is assigned to a port or LAG and you delete the CEE map, an error message displays in the **Status** area (applicable for the Traffic class map and ACL).

## Assigning a CEE map to a port or link aggregation group

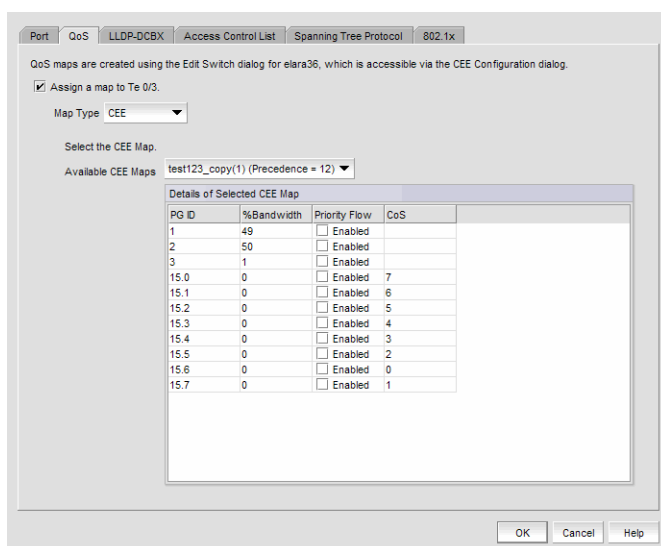
A port can have either a CEE map or a Traffic Class map assigned to it, but it cannot have both.

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the **QoS** tab on the **Edit Port** dialog box.

The **QoS** dialog box displays.



**FIGURE 182** QoS, Assign a CEE Map to a port dialog box

4. Click the **Assign a map to <port name>** check box.  
If you do not enable this check box, all QoS edit features are disabled.
5. Select **CEE Map** in the **Map Type** list.
6. Select a CEE Map in the **Available CEE Maps** list.  
If no CEE maps were created on the switch, the **Available CEE Maps** list is empty.
7. Click **OK** to commit the map assignment.  
The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Creating a traffic class map

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.  
The **QoS** dialog box displays.
4. Select **Traffic Class** from the **Map Type** list.
5. Name the Traffic Class map.
6. Click the Traffic Class cell in a CoS row and directly enter a value from 0-7. You can leave the cell empty to indicate zero (0).
7. Click the right arrow button to add the map to the **Traffic Class Maps** table.  
If the name of the Traffic Class map already exists, an overwrite warning message displays. Click **Yes** to overwrite the existing Traffic Class map.
8. Click **OK** if the Traffic Class map does not already exist.  
The **CEE Confirmation and Status** dialog box displays.
9. Review the changes carefully before you accept them.
10. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Editing a traffic class map

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.  
The **QoS** dialog box displays.
4. Select a Traffic Class Map from the **Traffic Class Maps** table, and click the left arrow button to load its values to the left pane. The fields are now editable.  
If the name of the Traffic Class map already exists, an overwrite warning message displays. Click **Yes** to overwrite the existing Traffic Class map.
5. Keep the same Traffic Class Map name and modify the values, as required.
6. Click the right arrow button to re-add the map to the Traffic Class Maps table.
7. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Deleting a traffic class map

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.  
The **QoS** dialog box displays.
4. Select a Traffic Class Map that you want to delete from the **Traffic Class Maps** table.
5. Click **Delete**.  
The **Delete confirmation** dialog displays.
6. Click **Yes** to confirm.  
The Traffic Class Map row is removed from the table.
7. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Assigning a traffic class map to a port or link aggregation group

You can assign a Traffic Class map to a port or ports under the LAG; however, a port does not *require* a Traffic Class map be assigned to it. A port can have either a CEE map or a Traffic Class map assigned to it, but it cannot have both.

---

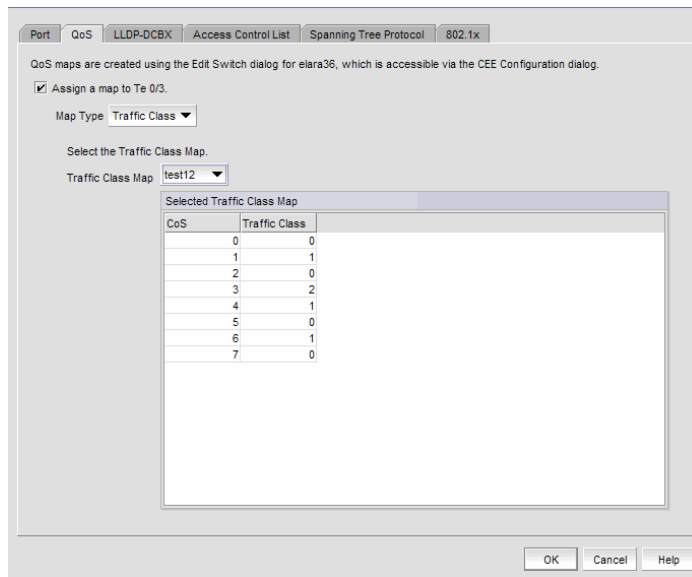
### NOTE

You cannot configure QoS or LLDP-DCBX on a LAG.

---

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a port or LAG, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.  
The **QoS** dialog box displays.

## 17 Assigning a traffic class map to a port or link aggregation group



**FIGURE 183** QoS, assign a traffic class map to a port dialog box

4. Click the **Assign a map to <port name>** check box.
5. Select **Traffic Class** in the **Map Type** list.
6. Select a Traffic Class Map in the **Traffic Class Map** list.
7. Click **OK** to commit the map assignment.

The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

# LLDP-DCBX configuration

Link Layer Discovery Protocol (LLDP) provides a solution for the configuration issues caused by increasing numbers and types of network devices in a LAN environment, because, with LLDP, you can statically monitor and configure each device on a network.

Data Center Bridging Capability Exchange Protocol (DCBX) enables Enhanced Ethernet devices to discover whether a peer device supports particular features, such as Priority Flow Control or Class of Service (CoS). In a Converged Enhanced Ethernet (CEE) environment, LLDP is enhanced with DCBX protocol to further share or change the configured CEE enhancements. You must enable the DCBX protocol and configure certain parameters in order to effectively utilize the benefits of a converged network.

Using the **LLDP-DCBX** dialog box, you can create and manage LLDP profiles and assign a LLDP profile to a port or link aggregation group (LAG).

## Configuring LLDP for FCoE

To configure LLDP for FCoE, complete the following steps.

1. Select **Configure > Switch > CEE**.  
The **CEE Configuration** dialog box displays.
2. Select the switch to edit in the **CEE Ports and LAGs** table and click **Edit**.  
The **CEE Edit Switch** dialog box displays.
3. Click the **LLDP-DCBX** tab.  
The **LLDP-DCBX** dialog box displays.

QoS LLDP-DCBX Access Control List Spanning Tree Protocol 802.1x

Create LLDP Profiles that will be available for assignment to ports on this switch.

☒ Enable LLDP-DCBX

**LLDP Profile**

Name:

Description:

Mode: Both Transmit and Receive

Hello(sec):  (Blank or 4-180)

Multiplier:  (Blank or 1-10)

Advertise:

- ☐ Port Description
- ☐ System Capabilities
- ☐ System Name
- ☐ System Description
- ☐ Management IP Address
- ☐ Dot1
- ☐ Dot3
- ☐ DCBX
- ☐ FCoE Application
- ☐ FCoE Logical Link

**LLDP Profiles**

| Name           | Description |
|----------------|-------------|
| Global Conf... |             |

Delete

**Details of Selected Profile**

|            |                         |
|------------|-------------------------|
| Mode       | Both Transmit and Recei |
| Hello      | 30                      |
| Multiplier | 4                       |
| Advertise1 |                         |
| Advertise2 |                         |
| Advertise3 |                         |
| Advertise4 |                         |
| Advertise5 |                         |
| Advertise6 |                         |

OK Cancel Help

**FIGURE 184** CEE Edit Switch dialog box - LLDP-DCBX tab

4. Select the **Global Configuration** LLDP profile in the **LLDP Profiles** table.
5. Click the left arrow button to edit.
6. Select the **FCoE Application** and **FCoE Logical Link** check boxes in the **Advertise** table to advertise them on the network.
7. Click **OK**.

The **CEE Confirmation and Status** dialog box displays.

8. Click **Start** on the **CEE Confirmation and Status** dialog box to save the changes to the switch.
9. Click **Close** on the **CEE Configuration** dialog box.

## Adding an LLDP profile

When LLDP is disabled on the switch, a yellow banner displays on the **LLDP-DCBX** dialog box, indicating that LLDP-DCBX is not only disabled on the switch, it is also disabled for all ports and LAGs on the switch.

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

The **LLDP-DCBX** dialog box displays.

4. Click the **Enable LLDP-DCBX** checkbox.
5. Configure the LLDP Profile parameters:
  - **Name** - Type a name for the LLDP profile.
    - ☐ If the name of the LLDP profile already exists on the switch, an overwrite warning displays.
    - ☐ You can change the <Global Configuration> name; when you click the right arrow button, a new LLDP is created.
  - **Description** - Type a meaningful description of the LLDP profile.
  - **Mode** - Select a mode from the list: Tx (transmitted) or Rx (received).
  - **Hello** - Enter a hello interval time for the bridge. The value range is 4-180 and the default value is 30.
  - **Multiplier** - Enter a multiplier. The value range is 1-10 and the default is 4.
  - **Advertise** - Check the profile parameters that you want to display as part of the LLDP profile:
    - Port description - The user-configured port description.
    - System name - The user-configured name of the local system.
    - System capabilities - The system capabilities running on the system.
    - System description - The system description containing information about the software running on the system.
    - Management IP address - The IP management address of the local system.
    - Dot 1..Dot 3 -

- DCBX - The DCBX profiles.
  - FCoE application - The FCoE application feature.
  - FCoE logical link - The logical link level for the SAN network.
6. Click the right arrow button to move the newly created profile into the DCBX Profiles table.
  7. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
  8. Review the changes carefully before you accept them.
  9. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Editing an LLDP profile

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.  
The **LLDP Profile** dialog box displays.
4. Select an LLDP Profile in the **LLDP Profile** table.

---

### NOTE

You can edit or rename the <Global Configuration> profile. You cannot, however, delete or duplicate global configurations.

---

5. Click the left arrow to load the LLDP Profile's values to the left pane.
6. Modify the values, as described in ["Adding an LLDP profile"](#) on page 446. You are not allowed to modify the LLDP Profile's name.
7. Click the right arrow to update the LLDP Profile parameters.
8. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
9. Review the changes carefully before you accept them.
10. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Deleting an LLDP profile

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.  
The **LLDP Profile** dialog box displays.

## 17 Assigning an LLDP profile to a port or ports in a LAG

4. Select an existing LLDP Profile from the **LLDP Profiles** table in the upper right pane.

---

### NOTE

You cannot delete <Global Configurations>. You can, however, edit global configurations. For more information, see [“Editing an LLDP profile”](#) on page 447

---

5. Click **Delete**.  
A confirmation dialog displays.
6. Click **Yes** to confirm you want to delete the LLDP profile.  
The **LLDP Profile** table row is removed.
7. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Assigning an LLDP profile to a port or ports in a LAG

You create LLDP profiles using the **Edit Switch** dialog box, which you access from the **CEE Configuration** dialog box. Global configuration parameters, which is the default selection, are displayed in the Assigned Profile table shown in [Figure 185](#).

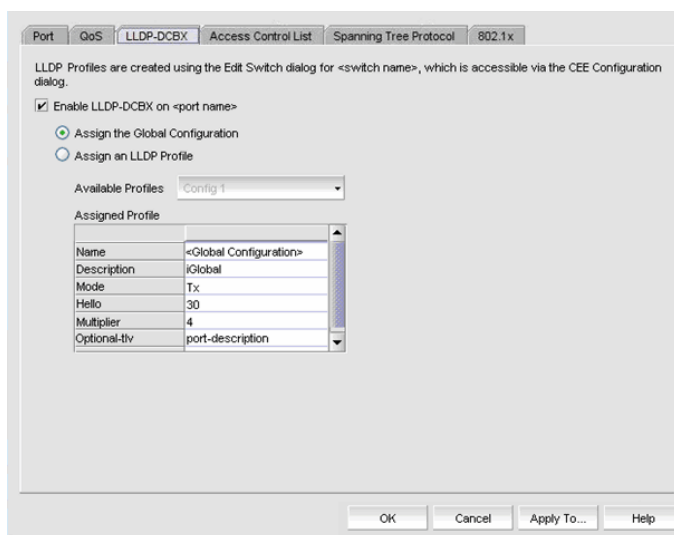
---

### NOTE

When LLDP is disabled on the switch, a yellow banner displays on the **LLDP-DCBX** dialog box, indicating that LLDP-DCBX is not only disabled on the switch, it is also disabled for all ports and LAGs on the switch.

---

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a port or link aggregation group (LAG), and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Port/Edit LAG** dialog box.  
The **Assign an LLDP profile to <port name>** dialog box displays.



**FIGURE 185** Assign an LLDP profile dialog box

4. Click **Assign an LLDP profile to <port name>** button to enable the feature.

---

**NOTE**

**Assign the Global Configuration** is the default. The **Available Profiles** list is disabled if global configuration is selected. In addition, the **Assign an LLDP profile** button is disabled if no LLDP profiles exist on the switch.

---

5. Select an LLDP profile from the **Available Profiles** list.
6. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
7. Review the changes carefully before you accept them. The port you selected on the **CEE Configuration** dialog box should now be assigned to the profile you selected from the **Available Profiles** list.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Access Control List configuration

Access control lists (ACL) are sequential lists consisting of permit and deny rules. They are either Layer 3 (IP)- or Layer 2 (MAC)-specific. You can configure multiple access lists and rules and store them in the configuration.

Some of the benefits of ACLs include the following:

- ACLs provide a measure of security.
- ACLs save network resources by reducing traffic.
- ACLs block unwanted traffic and users.
- ACLs reduce the chance of attacks.

You create an ACL on a switch and then you can apply the configuration to ports, and link aggregation groups (LAGs) on that switch.

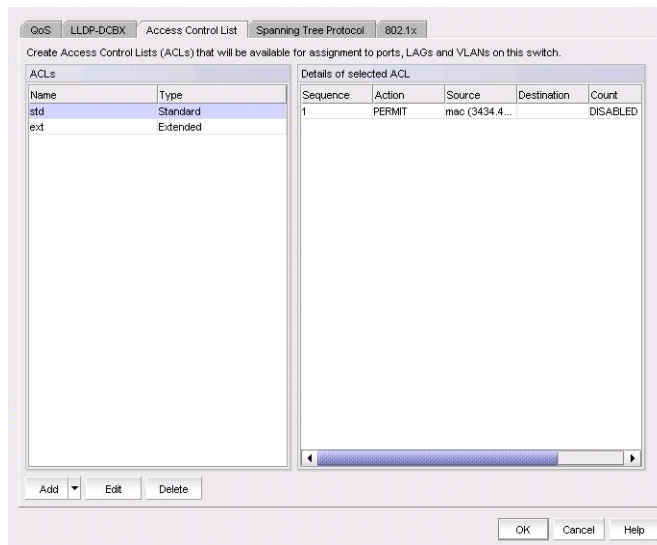
### Adding an ACL to a switch

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **Access Control List** tab on the **Edit Switch** dialog box.

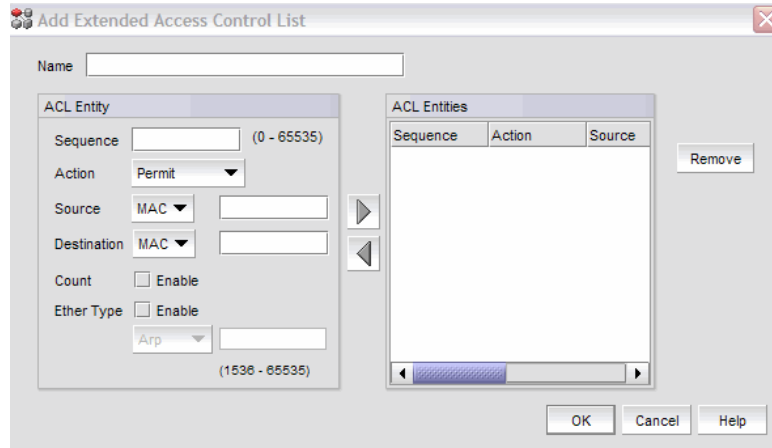
The **Access Control List** dialog box displays.



**FIGURE 186** Access Control List dialog box

4. Click **Add** and select **Standard** or **Extended** from the **Add** list.

The **Add Extended Access Control List** includes all the Standard ACL features plus two additional features: Destination and Ether Type. The ACL parameters are described below.



**FIGURE 187** Add Extended Access Control List dialog box

5. Configure the following Access Control List parameters.

#### NOTE

You cannot duplicate Action and Source parameters in an existing Standard ACL. You cannot duplicate Action, Source, Destination, and Ether Type parameters in an existing Extended ACL.

- **Sequence** - The sequence number that tracks all the ACL entities defined globally in the system. If you assign a Sequence number that is the same as an existing ACL Entity, an overwrite warning displays. After the overwrite operation, the system again checks for duplicates, then it creates the new ACL entity.
- **Action** - Select **Permit** or **Deny** from the list.
  - ☐ For a Standard ACL, the **Action** must be **Deny** and the **Source** must be **Any**.
  - ☐ For an Extended ACL, the **Action** must be **Deny** and the **Source** and **Destination** must be **Any**.
- **Source** - Enter the media access control (MAC) address where the packets originate. **Mask** is the subnet mask of the source MAC address. If you select "Any" from the **Source** list, the text box is cleared and disabled and the subnet mask is not applicable.

In the **Extended ACL** dialog box, you can select **Host** from the **Source** list, in addition to **MAC** or **Any**. If you select **Host** from the list, enter the host name where the packets originate.

- **Destination** - Enter the user-supplied packet destination MAC address. **Mask** is the packet subnet mask of the packet destination MAC address. If you select "Any" from the **Destination** list, the text box is cleared and disabled and the subnet mask is not applicable.

In the **Extended ACL** dialog box, you can select **Host** from the **Destination** list, in addition to **MAC** or **Any**. If you select **Host** from the list, enter the host name of the packet destination.

- **Count** - Instructs the system to maintain a counter.
- **Ether Type** - Specifies the Ethernet protocol being transferred in the Ethernet frame. Only one of the following Ether types is supported at a time.
  - ☐ **Address Resolution Protocol (ARP)** - Ether Type 0x0806
  - ☐ **Fibre Channel over Ethernet (FCoE)** - Ether Type 0x8906
  - ☐ **Internet Protocol, version 4 (IPv4)** - Ether Type 0x0800
  - ☐ **Custom** - Ether type values must be greater than or equal to 1536 (0x0600). The range is 1536 - 65535.

6. Click the right button to add the ACL entity to the **ACL Entities** table.

7. Click **OK** to close the dialog box. The newly-added ACL displays in the **ACL Entities** table.

If the name of the ACL already exists (duplicate Standard or Extended ACL names cannot exist), an overwrite warning message displays. Click **Yes** to overwrite the existing ACL.

If the name of the ACL does not already exist, the **CEE Confirmation and Status** dialog box displays.

8. Review the changes carefully before you accept them.

9. Click the **Start** button to apply the changes, or click **Close** to abort the operation.

You can now assign the ACL to ports or link aggregation groups (LAGs) on the switch.

## Editing the parameters of an ACL

You cannot change the name of the ACL (Standard or Extended) after you have created the ACL on the switch.

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.

3. Click the **Access Control List** tab on the **Edit Switch** dialog box.

The **Access Control List** dialog box displays.

4. Select an ACL row in the **ACLs** table and click **Edit**.

5. Modify the ACL parameters, as required, using the parameter descriptions in [“Adding an ACL to a switch”](#) on page 450.

6. Click **OK** to commit the ACL parameter changes.

The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.

8. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Deleting an ACL

When you delete an ACL from the **ACLs** table, you are given the option to also remove the profile from the entities where it is currently associated.

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **Access Control List** tab on the **Edit Switch** dialog box.

The **Access Control List** dialog box displays.

4. Select the ACL that you want to delete from the **ACLs** table.
5. Click **Delete**.

The selected ACL is removed from the ACLs table.

6. Click **OK** to commit the ACL parameter changes.

The **CEE Confirmation and Status** dialog box displays.

7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Assigning an ACL to a port or link aggregation group

An access control list (ACL) cannot be assigned to a port when the port is a member of a link aggregation group (LAG). An ACL can be assigned to a LAG, however.

---

### NOTE

The ports and the ports in a link aggregation group (LAG) for the selected switch must be in Layer 2 (L2) mode. If the ports or ports in a LAG are not in L2 mode, a yellow banner displays.

---

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

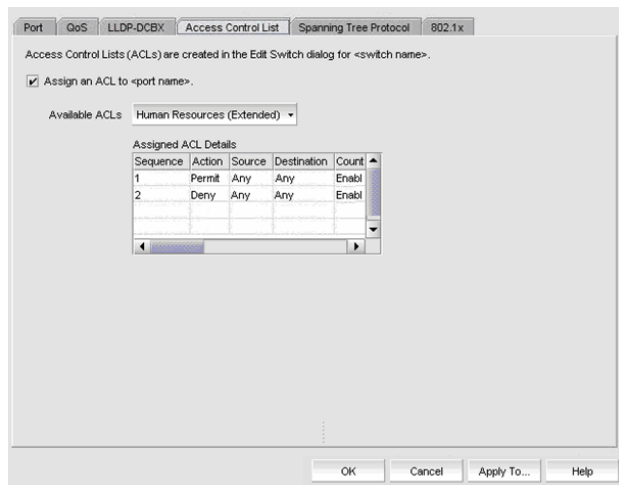
2. Select a port or LAG, and click **Edit**.
3. Click the **Access Control List** tab on the **Edit Port/Edit LAG** dialog box.

The **Access Control List** dialog box displays.

4. Click the **Assign Access Control List to <port name>** checkbox.

You can unassign an ACL by deselecting the **Assign an ACL to <port\_name>** checkbox.

## 17 Assigning an ACL to a port or link aggregation group



**FIGURE 188** Assign ACL to port dialog box

5. Select an ACL from the **Available ACLs** list.

The ACL name is suffixed with its type (standard or extended) in parentheses; for example, Human Resources (Extended). The details of the selected ACL are displayed in the Assigned ACL Details table, shown in [Figure 188](#).

6. Click **OK** to commit the assign the ACL to the port or LAG.  
The **CEE Confirmation and Status** dialog box displays.
7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Spanning Tree Protocol configuration

You can configure Spanning Tree Protocol (STP) when editing a LAG, but not when you are adding a LAG. The 8 Gbps 16-FC-ports, 10 GbE 8-Ethernet Port, and the 10 Gbps CEE/FC switch module support the following types of STP:

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP) - Provides for faster spanning tree convergence after a topology change. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.
- Multiple Spanning Tree Protocol (MSTP) - Provides support for virtual LANs (VLANs). This “per-VLAN” Multiple Spanning Tree Protocol configures a separate spanning tree for each VLAN group and blocks the links that are redundant within each spanning tree.

---

**NOTE**

STP is not supported for internal ports.

---

See [“Spanning Tree Protocol policy”](#) on page 427 for general information about Spanning Tree Protocol.

### Enabling Spanning Tree Protocol

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **Spanning Tree Protocol** tab on the **Edit Switch** dialog box.  
The **Enable Spanning Tree Protocol** dialog box displays.
4. Configure the Spanning Tree parameters, which are described in [“Setting Spanning Tree parameters for a switch”](#) on page 456.
5. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
6. Review the changes carefully before you accept them.
7. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Setting Spanning Tree parameters for a switch

You cannot configure Spanning Tree Protocol (STP) when adding a new LAG. STP can be configured only after the LAG has been added to the switch.

### NOTE

The ports and the ports in a link aggregation group (LAG) for the selected switch must be in Layer 2 (L2) mode. If the ports or ports in a LAG are not in L2 mode, a yellow banner displays, indicating Spanning Tree Protocol is disabled and the STP parameters are disabled as well.

1. Select **Configure > Switch > CEE** from the menu bar.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select a switch, and click **Edit**.

3. Click the **Spanning Tree Protocol** tab on the **Edit Port** dialog box.

The **Enable Spanning Tree Protocol** dialog box displays.

4. Click the **Enable Spanning Tree Protocol** check box to enable STP, and click **OK**.

The **Spanning Tree Protocol** dialog box displays.

**FIGURE 189** Spanning Tree Protocol dialog box, STP and RSTP

### NOTE

The phrase (currently enabled on switch) indicates which STP mode is configured on the switch.

5. Configure the following Spanning Tree Protocol parameters:

- **Priority** - The bridge priority. The value range is 0-61440 and the default value is 32768. The value must be in increments of 4096.
- **Mode** - The spanning tree protocol mode. Options include Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).
- **Forward Delay (sec)** - The forward delay for the bridge. The value range is 4-30 seconds and the default value is 15.
- **Hello Time (sec)** - The hello interval time for the bridge. The value range is 1-10 and the default value is 2.
- **Maximum Age (sec)** - The maximum time to listen in seconds. The value range is 6-40 and the default is 20 seconds. This feature is not available if running in MSTP mode.  
The maximum age has a range of  $[2 \times \text{Hello Time} + 1]$  to  $[2 \times \text{Forward Delay} - 1]$ . If you specify a Maximum Age value that exceeds this range, an error message displays.
- **Re-enable Port Interval** - The interval after which the port will be enabled. The value range is 10-1000000 and the default is 300.
- **Re-enable Port State** - Enables or disables the timeout mechanism for the port to be enabled back.
- **Path Cost** - Sets the path cost behavior. Options include Standard and Custom.

You can set additional STP parameters, listed below, on the selected switch if MSTP Spanning Tree Protocol is enabled, as shown in [Figure 190](#).

- **Cisco Interop** - Enables or disables Cisco interoperability.
- **Tx Hold Count** - Select the transmit hold count for the bridge. The value range is 1-10.
- **Max Hops** - Specify the number of hops in a region before the Bridge Protocol Data Units (BPDU) are discarded and the information held for a port is aged. The hop count determines when to trigger a reconfiguration. The value range is 1-40 and the default is 20.
- **Region** - The Multiple Spanning Tree (MST) region.
- **Revision** - The revision number for the configuration. The value range is 0-255 and the default is 0.

## 17 Setting Spanning Tree parameters for a switch

The image shows a configuration window titled 'Spanning Tree Protocol' with a tab labeled '802.1x'. The window contains the following settings:

- Additional Spanning Tree Protocol Parameters are set on this switch for Port and LAG levels.**
- ☒ **Enable Spanning Tree Protocol**
  - ☐ STP
  - ☐ RSTP (currently enabled on switch)
  - ☒ **MSTP**
- Switch Settings**
  - Priority:** 32,768 (range 0-61440)
  - Forward Delay (sec):** 15 (range 4-30)
  - Max Age (sec):** 20 (range 6-40)
  - Cisco Interop:** ☐ Enable
  - Re-enable Port interval:** 300 (range 10-1000000)
  - Re-enable Port state:** ☒ Enabled
  - Path Cost:** ☒ Standard, ☐ Custom
  - Tx Hold Count:** 10 (range 1-10)
  - Max Hops:** 20 (range 1-40)
  - Region:** (empty field)
  - Revision:** 0 (range 0-255)

Buttons at the bottom: OK, Cancel, Help.

**FIGURE 190** Spanning Tree Protocol dialog box, MSTP

6. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

## STP configurable parameters at the port or LAG level

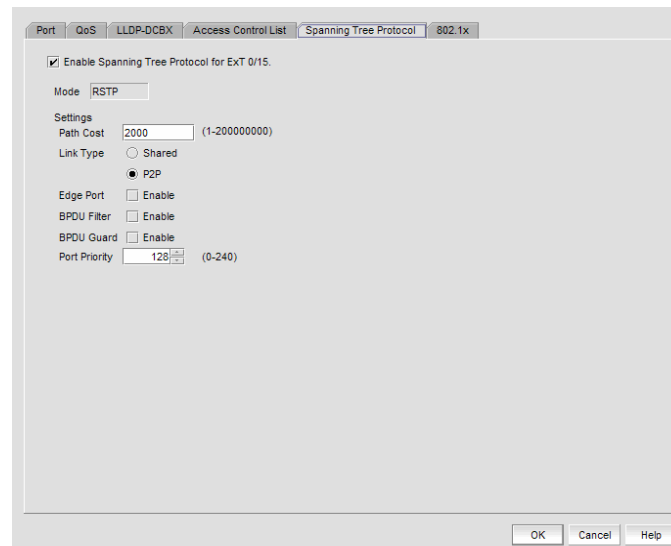
You cannot configure Spanning Tree Protocol (STP) when adding a new LAG. STP can be configured only after the LAG has been added to the switch.

Figure 191 shows the Spanning Tree Protocol (STP) parameters that are configurable at the port or LAG level.

The ports and the ports in a link aggregation group (LAG) for the selected switch must be in Layer 2 (L2) mode. If the ports or ports in a LAG are not in L2 mode, a yellow banner displays, indicating Spanning Tree Protocol is disabled and the STP parameters are disabled as well.

### NOTE

STP is not supported for internal ports on the 10 Gbps CEE/FC switch module. If an internal port is selected, the **Edit Port** dialog box and **Spanning Tree Protocol** tab do not display, and the L3 interface mode is unavailable.



**FIGURE 191** Spanning Tree Protocol dialog box, STP

You can configure the following Spanning Tree Protocol parameters.

- **Mode** - The spanning tree protocol mode.
- **Path Cost** - The port's path cost. The value range is 1 - 2000000000.
- **Link Type** - The link type for STP. Valid values are Shared or P2P.
- **Edge Port** - Enables the edge port to allow the interface to quickly transition to a forwarding state.
- **BPDU Filter** - Sets the portfast filter for the Bridge Protocol Data Units (BPDU). Valid values are Enable or Disable.
- **BPDU Guard** - Guards the port against the reception of BPDUs. Valid values are Enable or Disable.
- **Port Priority** - Port priority for MSTP. The value range is 0-240.

## 802.1x authentication

802.1x is a standard authentication protocol that defines a client-server-based access control and authentication protocol. 802.1x restricts unknown or unauthorized clients from connecting to a LAN through publicly accessible ports.

---

**NOTE**

802.1x is not supported for internal ports.

---

A switch must be enabled for 802.1x authentication before you configure its parameters. See [“Setting 802.1x parameters for a switch”](#) for more information.

### Enabling 802.1x authentication

802.1x authentication is enabled or disabled globally on the switch using the **Edit Switch** dialog box.

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch and click **Edit**.
3. Click the 802.1x tab on the **Edit Switch** dialog box.  
The **Enable 802.1x** dialog box displays.
4. Click the **Enable 802.1x** check box to enable 802.1x authentication, and click **OK**.  
The **802.1x** dialog box displays.
5. Configure the 802.1x parameters, which are described in [“Setting 802.1x parameters for a switch”](#) on page 461.
6. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Disabling 802.1x

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch and click **Edit**.
3. Click the 802.1x tab on the **Edit Switch** dialog box.  
The 802.1x dialog box displays.
4. Clear the **Enable 802.1x** check box to disable 802.1x authentication.
5. Click **OK**.  
The **CEE Confirmation and Status** dialog box displays.
6. Review the changes carefully before you accept them.
7. Click **Start** to apply the changes, or click **Close** to abort the operation.

## Setting 802.1x parameters for a switch

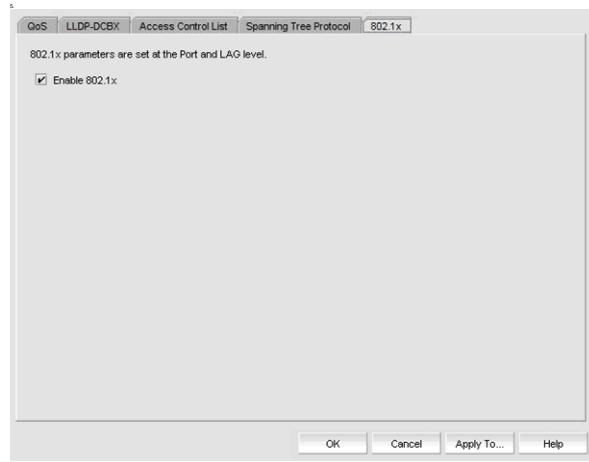
The 802.1x parameters can be configured whether the feature is enabled on the switch. The default parameters are initially populated when 802.1x is enabled, but you can change the default values as required.

1. Select **Configure > Switch > CEE** from the menu bar.  
The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.
2. Select a switch and click **Edit**.
3. Click the 802.1x tab on the **Edit Switch** dialog box.  
The **Enable 802.1x** dialog box displays.

## 17 Setting 802.1x parameters for a switch

4. Click the **Enable 802.1x** check box to enable 802.1x authentication, and click **OK**.

The **802.1x** dialog box displays.



**FIGURE 192** 802.1x dialog box

6. Configure the following 802.1x parameters:
  - **Wait Period** - The number of seconds the switch waits before sending an EAP request. The value range is 15 to 65535 seconds. The default value is 30.
  - **Retry Count** - The maximum number of times that the switch restarts the authentication process before setting the switch to an unauthorized state. The value range is 1 to 10. The default value is 2.
  - **Quiet Period** - The number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. The value range is 1 to 65535 seconds. The default value is 60.
  - **Re-authentication State** - Enable or disable the periodic re-authentication of the client. The default is Disable.
  - **Re-authentication Interval** - The number of seconds between re-authentication attempts. The value range is 1 to 4294967295. The default value is 3600 seconds. This feature is not dependent on the re-authentication state being enabled.
  - **Port Control** - Select an authorization mode from the list to configure the ports for authorization. Options include auto, force-authorized, or force-unauthorized and the default value is auto.
7. Click **OK**.

The **CEE Confirmation and Status** dialog box displays.
8. Review the changes carefully before you accept them.
9. Click **Start** to apply the changes, or click **Close** to abort the operation.

# CEE switch management using Web Tools

You can open Web Tools directly from the CEE Configuration dialog box and use the Element Manager to enable and manage the CEE switch.

To launch a CEE switch's Element Manager, complete the following steps.

1. Launch the CEE Configuration dialog box using one of the following methods:
- Select **Configure > Switch > CEE** from the menu bar.
  - Right-click the CEE switch from the device tree, and select **Configure > CEE**.
  - Right-click the CEE switch from the topology map and select **Configure > CEE**.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

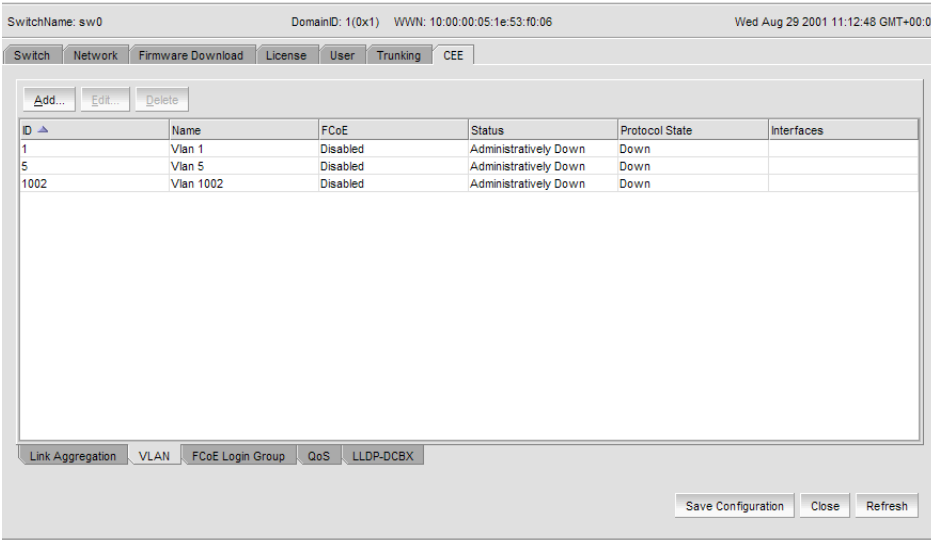
2. Select the CEE switch.

**NOTE**

For Fabric OS versions 6.3 and earlier, selecting a CEE switch launches the **Edit Switch** dialog box rather than the **CEE Configuration** dialog box.

3. Click **Element Manager**.

The Element Manager, shown in [Figure 193](#), launches automatically.



**FIGURE 193** Element Manager dialog box

For more information about Web Tools, refer to the *Brocade Web Tools Administrator's Guide*.

## CEE switch management using Telnet

You can use Telnet to log in and issue command line-based commands to a CEE switch.

To launch a Telnet session, complete the following steps:

1. Launch the CEE Configuration dialog box using one of the following methods:

- Select **Configure > Switch > CEE** from the menu bar.
- Right-click the CEE switch from the device tree, and select **Configure > CEE**.
- Right-click the CEE switch from the topology map and select **Configure > CEE**.

The **CEE Configuration** dialog box displays, showing the status of all CEE-related hardware and functions.

2. Select the CEE switch.
3. Click **Telnet**.

The Telnet session window displays.

---

**NOTE**

On Linux systems, you must use CTRL + BACKSPACE to delete text in the Telnet session window.

---

## Virtual FCoE port configuration

The virtual FCoE port has the following configuration features:

- Eight 10-Gbps CEE ports, which can be enabled for FCoE traffic.
- One-to-one mapping of FCoE ports with 10 Gbps Ethernet ports.
- Eight 8 Gbps FC ports.
- 24 internal FCoE ports, which provide the Ethernet-to-FC bridging capability. You can enable or disable each FCoE trunk individually.
- Each of the FCoE ports can be configured as an E\_Port or an F\_Port.

## Viewing virtual FCoE ports

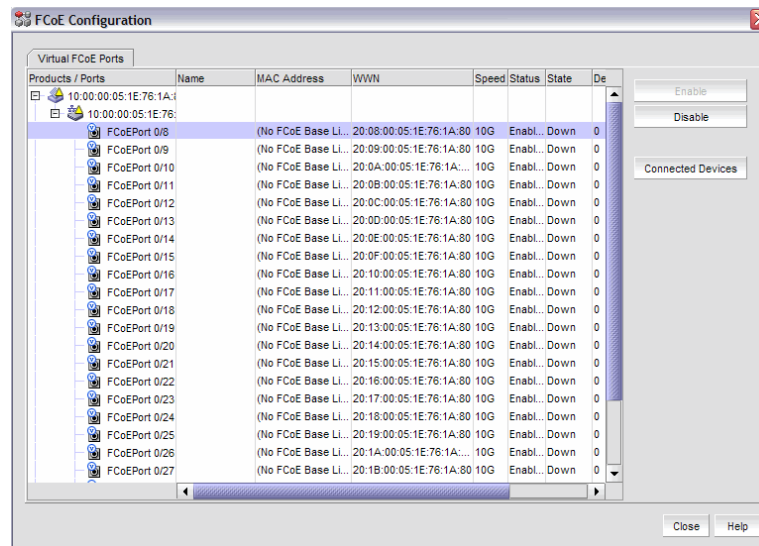
Configuration of virtual FCoE ports requires installation of the FCoE license on the switch.

1. Select **Configure > Switch > FCoE** from the menu bar.

The **FCoE Configuration** dialog box displays.

2. Select the **Virtual FCoE Ports** tab.

The **Virtual FCoE Ports** tab displays.



**FIGURE 194** Virtual FCoE Ports dialog box

3. Select one or more virtual ports from the **Products/Ports** list.
4. Perform one of the following tasks:
  - Click **Enable** to enable a selected virtual FCoE port for CEE configuration.
  - Click **Disable** to disable a selected virtual FCoE port from CEE configuration.
  - Click **Connected Devices** to view a list of FCoE virtual ports and to what they are directly connected.
5. Click **Close** to close the dialog box.

## Clearing a stale entry

A stale entry is a device that logged in and logged off but, because a port went down after an FLOGI was received, the device failed to receive the message. The entry in the **FCoE Connected Devices** table becomes stale and you must clear it manually.

1. Select a virtual FCoE port from the **FCoE Configuration** dialog box and click **Connected Devices**.

The **Connected Devices** dialog box displays.

2. Select one or more rows from the **Connected Devices** table and click **Disconnect**.

The **CEE Confirmation and Status** dialog displays.

3. Click **OK**.

The selected connected device should be cleared from the switch cache and from the table.

Note, however, that the connected devices might still be active and this operation could potentially stop traffic between the connected devices and the switch.

4. Review the changes carefully before you accept them.
5. Click **Start** to apply the changes, or click **Close** to abort the operation.

On closing the CEE Confirmation and Status dialog box, the **FCoE Configuration** Dialog refreshes the data and the latest information about the FCoE ports are displayed.

# FICON Environments

---

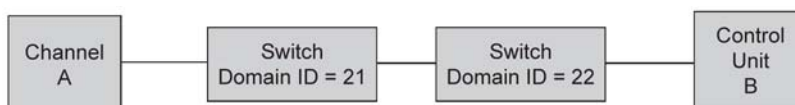
## In this chapter

- FICON Configurations ..... 467
- Configuring a PDCM Allow/Prohibit Matrix ..... 468
- Copying a PDCM configuration ..... 471
- Activating a PDCM configuration ..... 474
- Deleting a PDCM configuration ..... 475
- Changing the PDCM matrix display ..... 475
- Configuring a cascaded FICON fabric. .... 477
- Merging two cascaded FICON fabrics ..... 480
- Port Groups ..... 483
- Swapping blades ..... 486

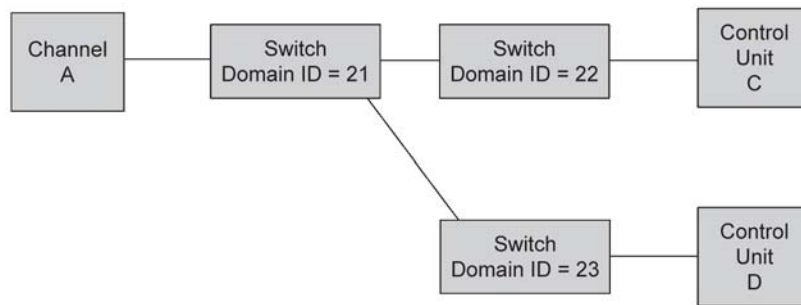
## FICON Configurations

IBM Fibre Connection (FICON) is a protocol used between IBM (and compatible) mainframes and storage. FICON configurations can be categorized into three types, based on complexity:

- Point-to-point configurations that do not use a switch.
- Switched point-to-point configurations, also called single switch configurations, connect a host channel to a storage control unit using a single switch. In this type of configuration, the channel is configured to use single-byte addressing.
- Cascaded configurations, also called high integrity fabrics, connect host channels and storage control units that reside in different domains. Cascaded FICON fabrics must be configured as high integrity fabrics. In this type of configuration, the channel is configured to use two-byte link addressing. [Figure 195](#) and [Figure 196](#) are examples of cascaded FICON configurations. IBM does not support configurations that have more than two domains in a path from a FICON Channel interface to a FICON Control Unit interface to CTC except under special circumstances.



**FIGURE 195** Cascaded configuration, two domains



**FIGURE 196** Cascaded configuration, three domains, but only two in a path

## Configuring a PDCM Allow/Prohibit Matrix

The Prohibit Dynamic Connectivity Mask (PDCM) is a FICON port attribute that can be used to prohibit communication between specific ports. Prohibits are not recommended on E\_Ports (inter switch links).

The PDCM can be manipulated by host-based management programs using FICON CUP, or from a Management program to create policies and determine paths for data and command flows. Up to 8 PDCM matrices can be modified at the same time. PDCM settings apply per switch rather than per fabric, and only work when an active zone configuration is present in the fabric.

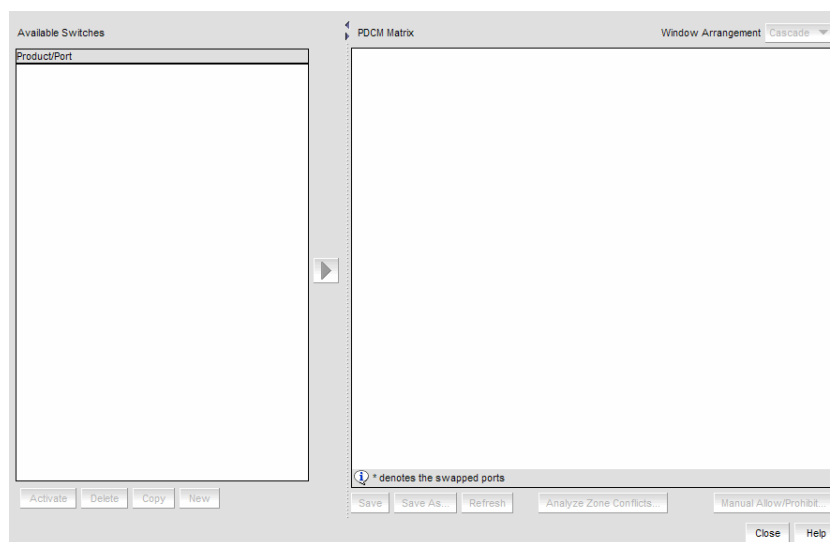
Multiple configurations may be defined, edited, copied, or removed. Only one configuration may be active per switch.

### NOTE

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

1. Select **Configure > Allow/Prohibit Matrix**.

The **Configure Allow/Prohibit Matrix** dialog box displays.



**FIGURE 197** Configure Allow/Prohibit Matrix dialog box

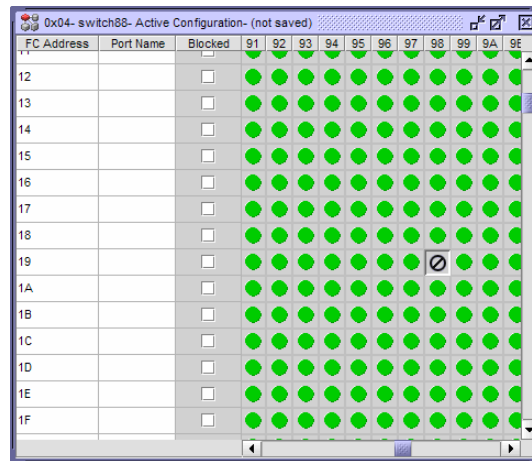
2. Select a switch from **Available Switches**.

Two default configurations (Active and IPL) are displayed in a tree structure below the switch. Existing configurations are also displayed.

3. Choose one of the following options:

- Double-click a configuration file.
- Select a configuration file and click the right arrow.

A matrix displays. The switch ports are displayed on both the vertical axis and horizontal axis. A green circle icon (●) indicates communication is allowed between the ports.



**FIGURE 198** Active Configuration

4. Prohibit a connection between two ports by clicking the intersection point between the ports.

A prohibit icon (⊘) displays at the intersection point. If you know the port addresses of the ports for which you want to prohibit or allow communication and do not want to search the matrix for the exact port intersection point, use the procedure [“Configuring an Allow/Prohibit manually”](#) on page 470.

5. Repeat step 4 as needed to create the matrix you want to apply. If you want to change a selection from prohibit to allow, click the intersection point to clear the prohibit icon.
6. When you have completed the matrix, click **Save** if you started with a new matrix, or **Save As** to save a copy of an existing matrix.
7. Click **Analyze Zone Conflicts**.

This operation can be done before or after a configuration is saved. This operation checks the current zoning settings for conflicts with settings in the PDCM matrix. Zone conflict is analyzed against the switch for port zoning only. The table cells display in the red background if the two ports are not in the same zone in an active zone configuration.

8. Click **Close** on the **Configure Allow/Prohibit Matrix** dialog box.

## Configuring an Allow/Prohibit manually

### NOTE

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

To configure to allow or prohibit communication between specific ports manually, complete the following steps.

1. Select **Configure > Allow/Prohibit Matrix**.

The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select a switch from **Available Switches**.

Two default configurations (Active and IPL) are displayed in a tree structure below the switch. Existing configurations are also displayed.

3. Choose one of the following options:

- Double-click a configuration file.
- Select a configuration file and click the right arrow.

A matrix displays. The switch ports are displayed on both the vertical axis and horizontal axis. A green circle icon (●) indicates communication is allowed between the ports.

4. Click **Manual Allow/Prohibit**.

The **Manual Allow/Prohibit** dialog box displays.

**FIGURE 199** Manual Allow/Prohibit dialog box

5. Select one of the following options
  - Select **Allow** to allow communication between two specific ports.
  - Select **Prohibit** to prohibit communication between two specific ports.
6. Enter the port number of the first port for which you want to allow or prohibit communication in the **Port Address 1** field.
7. Enter the port number of the second port for which you want to allow or prohibit communication in the **Port Address 2** field.

8. Click **Add**.

The information displays in the **Selected Ports for Modification** table.

To delete any of these manual configurations, select the configuration you want to delete in the **Selected Ports for Modification** table and click **Remove**.

9. Repeat steps [step 5](#) through [step 8](#) for each Allow/Prohibit configuration.
10. Click **OK** on the **Manual Allow/Prohibit** dialog box.
11. When you have completed the matrix, click **Save** if you started with a new matrix, or **Save As** if you edited a copy of an existing matrix.
12. Click **Analyze Zone Conflicts**.

This operation can be done before or after a configuration is saved. This operation checks the current zoning settings for conflicts with settings in the PDCM matrix. Zone conflict is analyzed against the switch for port zoning only. The table cells display in the red background if the two ports are not in the same zone in an active zone configuration.

13. Click **Close** on the **Configure Allow/Prohibit Matrix** dialog box.

## Saving or Copying a PDCM configuration to another device

When copying or saving a configuration from a small switch (source switch with fewer ports; for example, 64 ports) to a larger switch (destination switch with a larger number of ports; for example, 256 ports) only the port address range of the smaller switch will be affected on the larger switch. All additional port addresses will display the default settings (port state defaults to 'Allow' and the Blocked check box defaults to not checked).

Copying or saving a configuration from a larger switch to a smaller device only copies or saves the port address range that matches the smaller switch. Additionally a message displays that the additional port addresses from the larger switch are discarded.

When copying or saving a configuration from or to Logical Switches, the only ports affected are the port addresses defined in the Logical Switch. The FICONd CUP Daemon retains the full compliment of records regardless of the size of the Logical Switch. Therefore, copying or saving a configuration from or to logical switches should work the same as copying or saving between standard switches.

### Copying a PDCM configuration

---

#### NOTE

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

---

To duplicate an existing PDCM configuration, complete the following steps.

1. Select **Configure > Allow/Prohibit Matrix**.

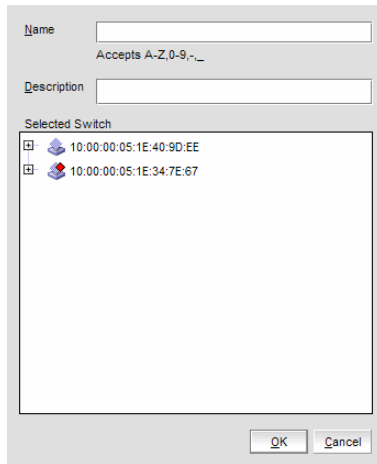
The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select the PDCM configuration you want to copy.

You can do this by expanding the view for the switch under **Available Switches** and selecting a configuration, or you may select the matrix under **PDCM Matrix**.

## 3. Click **Copy**.

The Save As/Copy dialog box displays.



**FIGURE 200** Save As/Copy dialog box

4. Enter a name for the configuration.
5. Enter a description for the configuration.
6. Select the check box for the switch to which you want to save the configuration in the **Select Switch** table.
7. Click **OK**.

A message displays stating that the outstanding port configuration is discarded when copying a configuration from the switch with more ports to a switch with fewer ports and vice versa. Click **OK** to close the message.

The copied configuration displays in the **Available Switches** table under the selected switch. To edit this configuration, refer to [“Configuring a PDCM Allow/Prohibit Matrix”](#) on page 468 or [“Configuring an Allow/Prohibit manually”](#) on page 470.

## Saving a PDCM configuration to another device

### NOTE

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

To save an existing PDCM configuration to another device, complete the following steps.

1. Select **Configure > Allow/Prohibit Matrix**.

The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select the PDCM configuration you want to copy.

You can do this by expanding the view for the switch under **Available Switches** and selecting a configuration, or you may select the matrix under **PDCM Matrix**.

3. Click **Save As**.

The Save As/Copy dialog box displays.

| Selected Switch          |                         |
|--------------------------|-------------------------|
| <input type="checkbox"/> | 10:00:00:05:1E:40:9D:EE |
| <input type="checkbox"/> | 10:00:00:05:1E:34:7E:67 |

**FIGURE 201** Save As/Copy dialog box

4. Enter a name for the configuration.
5. Enter a description for the configuration.
6. Select the check box for the device to which you want to save the configuration in the **Select Switch** table.
7. Click **OK**.

A message displays stating that the outstanding port configuration is discarded when copying a configuration from the switch with more ports to a switch with fewer ports and vice versa. Click **OK** to close the message.

The saved configuration displays in the **Available Switches** table under the selected switch. To edit this configuration, refer to [“Configuring a PDCM Allow/Prohibit Matrix”](#) on page 468 or [“Configuring an Allow/Prohibit manually”](#) on page 470.

## Activating a PDCM configuration

### NOTE

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

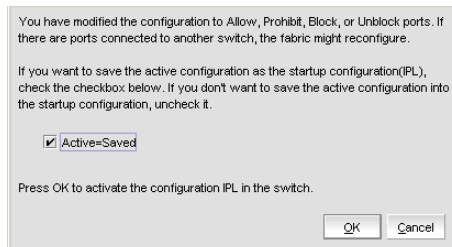
You must have an active zone configuration before you can activate a PDCM configuration.

1. Select **Configure > Allow/Prohibit Matrix**.

The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select the PDCM configuration you want to activate. You can do this by expanding the view for the switch under **Available Switches** and selecting a configuration, or you may select the matrix under **PDCM Matrix**.
3. Click **Activate**.

A confirmation message displays.



**FIGURE 202** Activate Matrix Confirmation message

4. Select the **Active=Saved** check box to save the active configuration as the startup configuration (IPL).
5. Click **OK** to confirm.

If you select the **Active=Saved** check box, the text [=Active] is appended to the IPL file in the **Configure Allow/Prohibit Matrix** dialog box.

The **Active=Saved** check box and IPL filename represent the current state of the Active=Saved Mode (ASM) bit on the switch. However, this is limited to changes done to the ASM configuration through the Management application. If changes occur through external means (such as, Webtools/CLI) the changes are not reflected in the Management application until the PDCM dialog box is re-launched.

## Deleting a PDCM configuration

---

**NOTE**

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

---

You cannot delete the active configuration, the IPL configuration, or a configuration that is marked as having uncommitted changes.

1. Select **Configure > Allow/Prohibit Matrix**.

The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select the PDCM configuration you want to delete. You can do this by expanding the view for the switch under **Available Switches** and selecting a configuration, or you may select the matrix under **PDCM Matrix**.

3. Click **Delete**.

A confirmation message displays.

4. Click **Yes** to confirm.

## Changing the PDCM matrix display

---

**NOTE**

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

---

There are three options for the **PDCM Matrix** display on the **Configure Allow/Prohibit Matrix** dialog box:

- The matrix definitions may be cascaded (this is the default view).
- The matrix definitions may be tiled horizontally.
- The matrix definitions may be tiled vertically.

Perform the following steps to change the display to the desired format.

1. Select **Configure > Allow/Prohibit Matrix**.

The **Configure Allow/Prohibit Matrix** dialog box displays.

2. Select **Cascade**, **Tile Horizontally**, or **Tile Vertically** from the **Window Arrangement** list.

## Cascaded FICON fabric

---

**NOTE**

You must have FICON Management privileges to configure a fabric for cascaded FICON.

---

The Management application enables you to easily configure a fabric for cascaded FICON. Note that configuring a fabric for cascaded FICON may be disruptive to current I/O operations in the fabric, as it needs to disable and enable the switches in the fabric.

FICON configuration performs the following operations on the selected fabric:

- Turns on the insistent domain ID flag (IDID) on all switches.
- Sets High Integrity Fabric Configuration (HIFC) on the seed switch.
  - Fabric-wide consistency policy is configured to include SCC in strict mode.
  - SCC policy is created or modified to limit connectivity to only the switches in the selected fabric.
- Enables port-based routing on 4 Gbit/sec platform switches.
- Enables In-Order Delivery (IOD) on all switches.
- Disables Dynamic Load Sharing (DLS) on all switches.
- (Optional) Turns on FICON Management Server (FMS) mode on all switches.

If some switches already have FMS mode enabled, it is re-enabled. If you select FMS mode to be enabled on all switches and if some of the switches do not have a CUP license, then after successful configuration, you can access the Port Connectivity (PDCM) matrix, but the host system cannot communicate with the FICON Management Server unless you install a CUP license. If a CUP license is later installed on these switches, then FMS mode must be re-enabled on these switches.

If there are any M-EOS switches in the selected fabric, configuration enables Enterprise Fabric Mode (EFM) on those switches.

## Configuring a cascaded FICON fabric

### NOTE

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

The FICON wizard automatically creates high integrity fabric configuration settings that support a cascaded FICON fabric.

1. Select **Configure > FICON > Configure Fabric**.

The **Configure Cascaded FICON Fabric** screen of the FICON Configuration dialog displays (Figure 203).

Select a fabric to configure for cascaded FICON from the listed fabrics that support this utility. DLS cannot be enabled, if none of the switches in the fabric support lossless DLS.

Fabric: 10:00:00:05:1E:34:DF:35 (10.32.149.10)

FMS Mode: ☐ Enable 256 Area Assignment: Disable

DLS: ☐ Enable

Routing: ☒ Port-Based ☐ Exchange-Based

**Warning:** The configuration may disturb the current I/O in the fabrics, it needs to disable/enable the switches in the fabric. It is recommended to take a configuration backup of all switches before clicking on "OK" to perform the operation. This will help to revert back the switch configuration later.

The Configuration will perform the following actions:

- Turn on insistent domain ID (IDID) on all switches.
- Set High Integrity Fabric Configuration - Set Switch Connection Control Policies on all switches to limit connectivity to only the switches in the selected fabric.
- Enable Port-Based Routing on 4/8 GB/s platform switches.
- Enable In Order Delivery (IOD) on all switches.
- Disable Dynamic Load Sharing (DLS) on all switches.
- Optionally, turn on FICON Management Server (FMS) mode on all switches in the fabric. This feature must be enabled on a switch to allow Control Unit Port (CUP) management features and it requires a CUP license. If enabled, an Active Zone Configuration is required for the PDCM to take effect.
- If there is any m-EOS switch in the selected fabric, Enterprise Fabric Mode (EFM) will be enabled on that switch.

OK Cancel Help

**FIGURE 203** Configure Cascaded FICON Fabric dialog box

2. Use the **Fabric** drop-down selector to select the fabric you want to configure.

### NOTE

(Fabric OS switches only) All switches in a fabric must be running Fabric OS version 5.2 or later. If a Fabric OS version earlier than version 5.2 is present in the topology, the fabric is not listed.

3. Select the **FMS Mode** check box to manage the fabric by a host-based management program using FICON CUP protocol.

If you select **FMS Mode**, each switch is checked for a CUP license. Any switches that do not have a CUP license are listed, with a reminder that a CUP license is necessary to communicate with the fabric management server.

4. Select the **DLS** check box to enable dynamic load sharing (DLS) or Lossless DLS on all switches in the fabric.

---

### NOTE

DLS requires DLS support on the switch. Lossless DLS requires Lossless DLS support on the switch.

---

DLS is only supported on the 40-port, 8 Gbps FC Switch, 80-port, 8 Gbps FC Switch, 384-port Backbone Chassis, and 192-port Backbone Chassis.

Enabling DLS may result in dropped frames when paths fail over. It is recommended that you set the preferred IOD Delay Time to minimize frame drops.

5. Select to enable port-based or exchange-based routing on switches.

If you select **Port-Based Routing**, enables port-based routing on 4 Gbps platform switches.

If you select **Exchange-Based Routing**, enables exchange-based routing on 8 Gbps platform switches running Fabric OS 6.4 or later. Enables port-based routing on all other switches in the fabric.

6. Choose one of the following options from the **256 Area Assignment** list:

- **Disabled**—select to disable the 256 Area Assignment addressing mode.

Disabling the 256 Area Assignment mode assigns an area to every port with no imposed limit. This is the default.

- **Zero Based Area Assignment**—select to use zero based area assignment.

Zero Based Area Assignment mode assigns areas as ports are added to the partition, beginning at area zero. This mode allows FICON customers to make use of the upper ports of a high density blade; but this mode may not be compatible with domain,index zoning in InteropMode 2, because M-EOS switches are not capable of handling indexes greater than 255.

- **Port Based Area Assignment**—select to use port based area assignment.

Port Based Area Assignment mode matches the port index to the area assignment. You cannot use high density blades if you select this option.

7. Click **OK** if you want to proceed after reading the warning and bulleted items.
8. A warning message displays explaining that SCC and DCC policies will be created and activated on the fabric. Click **Yes** to continue.

If configuration is successful, a confirmation message displays.

If **FMS Mode** was selected, each switch is checked for a CUP license. Any switches that do not have a CUP license are listed, with a reminder that a CUP license is necessary to communicate with the fabric management server.

## Cascaded FICON fabric merge

The Management application provides a wizard to help you merge two fabrics for cascaded FICON. Note that merging two cascaded FICON fabrics may be disruptive to current I/O operations in both fabrics, as it needs to disable and enable the switches in both fabrics.

---

### NOTE

It is recommended that you run a configuration backup on all switches before performing the fabric merge. This helps you to revert back the switch configurations later.

---

The cascaded FICON merge wizard performs the following operations on the selected fabrics:

- Checks the fabrics for any merge issues.
- Turns on the insistent domain ID (IDID) flag on all of the switches in both fabrics.
- Clears Admin Domain, Access Control Lists (ACLs), and zone databases, if they exist, from one of the fabrics (you select which fabric from within the wizard).

---

### NOTE

Clearing the ACL database in a large fabric might take a long time; for example, in a 50-switch fabric, this operation might take from 30 minutes to 1 hour.

---

- Configures High Integrity Fabric Configuration (HIFC) on the seed switch of the primary fabric.
  - Fabric-wide consistency policy is configured to include SCC in strict mode.
  - SCC policy is created or modified to limit connectivity to only the switches in both fabrics.
- Enables port-based or exchange-based routing on switches.
  - If you select Port-Based Routing, enables port-based routing on 4 Gbit/sec platform switches.
  - If you select Exchange-Based Routing, enables exchange-based routing on 8 Gbit/sec platform switches running Fabric OS 6.4 or later. Enables port-based routing on all other switches in the fabric.
- Enables or disables Dynamic Load Sharing (DLS) on all switches.
  - If you select Enable DLS, performs the following actions:
    - ☐ Enables In-Order Delivery (IOD) with lossless DLS on switches that support lossless DLS and enables IOD without lossless DLS on all other switches.
    - ☐ Enables DLS on switches that support lossless DLS and disables DLS on all other switches.
  - If you do not select Enable DLS, performs the following actions:
    - ☐ Enables IOD on all switches.
    - ☐ Disables DLS on all switches.
- (Optional) Turns on FICON Management Server (FMS) mode on all switches. If some switches already have FMS mode enabled, it is re-enabled.
 

If you select FMS mode to be enabled on all switches and if some of the switches do not have a CUP license, then after successful configuration, you can access the Port Connectivity (PDCM) matrix, but the host system cannot communicate with the FICON Management Server unless you install a CUP license. If a CUP license is later installed on these switches, then FMS mode must be re-enabled on these switches.
- (Optional) Configures long distance settings on selected ports (requires Extended Fabric license).

## Merging two cascaded FICON fabrics

---

### NOTE

If you receive a 'FICON not supported on switch' error, refer to FICON troubleshooting for a list of possible causes.

---

If you want to join two cascaded FICON fabrics, they must be merged. If the distance between fabrics is 10 km or more, an Extended Fabrics license is required, and an extra step is required to configure the connection as a long distance connection. To successfully configure a long distance connection, use the same E\_Ports and cable distance values used when configuring Extended Fabrics. For long distance connections, it is recommended that you create the Extended Fabrics configuration first, have an active connection, and have the E\_port and cable distances values ready before you merge the fabrics.

1. Select **Configure > FICON > Merge Fabrics**.

The **Overview** screen of the **Cascade FICON Fabrics Merge** wizard displays.

2. Click **Next**.

The **Select fabrics** screen displays.

3. Select the two fabrics you want to merge under **Available Fabrics**, and click the right arrow to move them to **Selected Fabrics**. You may do this one fabric at a time, or select both by pressing CTRL and then clicking each fabric.

---

### NOTE

All switches in a fabric must be running OS version 5.2 or later and must be reachable. If a Fabric OS version earlier than version 5.2 is present in the fabric, the fabric is not listed.

---

4. Click **Next**.

The **Set up merge options** screen displays.

5. Select **FMS Mode** to manage the fabric by a host-based management program using FICON CUP protocol.
6. Select the **DLS** check box to enable dynamic load sharing (DLS) or Lossless DLS on all switches in the fabric.

---

### NOTE

DLS requires DLS support on the switch. Lossless DLS requires Lossless DLS support on the switch.

---

DLS is only supported on the 40-port, 8 Gbps FC Switch, 80-port, 8 Gbps FC Switch, 384-port Backbone Chassis, and 192-port Backbone Chassis.

Enabling DLS may result in dropped frames when paths fail over. It is recommended that you set the preferred IOD Delay Time to minimize frame drops.

7. Select to enable port-based or exchange-based routing on switches.

If you select **Port-Based Routing**, enables port-based routing on 4 Gbit/sec platform switches.

If you select **Exchange-Based Routing**, enables exchange-based routing on 8 Gbit/sec platform switches running Fabric OS 6.4 or later. Enables port-based routing on all other switches in the fabric.

8. Select which fabric's Administrative domains, zone database, and ACL database you want to preserve and use after the fabrics are merged.
9. Read the bulleted list of actions so you understand the actions that are taken to avoid conflicts when the fabrics are merged.
10. Click **Next**.

The **Check merge** screen displays.

A **Status details** table shows progress through merge check points. A rotating arrow under **Status** indicates a **Merge check** step is in progress. A blue check mark indicates successful completion of that **Merge check**. A red stop sign indicates a failed step. If the configuration is successful, all configuration items have blue check marks.

11. Click **Next** to continue.

The **Configure long distance (optional)** dialog box displays. If the distance between the merged fabrics is 10 km or greater, you must configure the connection as a long distance connection. Selecting a distance invokes an algorithm to compute the required number of BB Credits available to the port. The longer the link, the greater latency, resulting in the potential for more outstanding frames in the link, and the need for more BB credits. FICON may require more BB credits than the algorithm provides, and it is a good practice to specify a distance that is longer than the actual distance to be sure enough BB credits are allocated.

12. Perform the appropriate following action based on whether the connection is a long distance connection or not:
  - If it is not a long distance connection, click **Next** to view the **Configure merge** screen. Proceed to [step 13](#).
  - If it is a long distance connection, expand the fabrics under **Selected Fabrics** to the switch port level.
    - a. Select the E\_ports used for the connection on the local switch and on the remote switch, and click the right arrow.  
The selected E\_ports are moved to **Selected Ports**.  
If there is no E\_port in the selected fabrics, a warning message displays.
    - b. Specify the **Cable length between switch ports**.  
The default value is 50 km, and the range is 10 to 500 km.
    - c. Select **ARBs** or **IDLEs** to configure the **Fibre Channel Primitive Signal Fill Words**.  
For Fabric OS version 6.1.0b or earlier, the setting is always ARBs. You cannot change to IDLEs.  
For Fabric OS version 6.1.0c or later, the default setting is IDLEs, however, you can change it to ARBs.
    - d. Click **Next**.  
The **Configure merge** screen displays.
13. Read and review the information on the **Configure merge** screen. If you understand and agree, click **Next** to confirm the information.  
A **Summary** screen displays.
14. Read the information, and click **Finish** to dismiss the wizard.

## Resolving merge conflicts

You can resolve the following types of switch configuration conflicts:

- Domain ID
- TOV
- Buffer To Buffer Credit
- Disable Device Probe
- Route Priority Per Frame
- Sequence Level Switching
- Suppress Class F
- Long Distance Setting
- Data Field Size
- VC Priority

Note that not all tests support resolution. If a test supports resolution, the **Description** column contains the text 'Resolvable'.

To resolve merge conflicts, complete the following steps.

1. Select the failed test where the **Description** column contains the text 'Resolvable'.
2. Click **Resolve**.

A “The switches in fabric *Name* will be disabled prior to making the configuration change. The switches will be reenabled after the configuration changes are applied. Please confirm to proceed.” warning message displays.

3. Click **OK** on the warning message.

The values of the Fabric chosen on the **Set up merge options** screen are applied to all devices in the second fabric. Once the settings are applied the test is run again and the merge results are updated.

If the test passes, go to [step 4](#).

If an error occurs, an error message displays. You must use Web Tools or the CLI to resolve this conflict. Click **OK** on the error message and go to [step 4](#).

If you are resolving a domain ID error, there may be multiple switches involved. If multiple switches have the domain ID error, the **Configure Domain IDs** dialog box displays listing all devices that have domain ID conflict.

- a. Select the device you want to resolve the domain ID for in the **Available Switches** table and click the right arrow button.
  - b. Select a new domain ID for the device from the **Domain ID** list.
  - c. Repeat steps a and b for each device in the **Available Switches** table.
  - d. Click **OK** on the **Configure Domain IDs** dialog box.
4. Repeat [step 1](#) through [step 3](#) until all resolvable tests pass.
  5. Perform [step 11](#) through [step 14](#) of the procedure “[Merging two cascaded FICON fabrics](#)” on page 480 to finish resolving a merge conflict.

# Port Groups

A port group is a group of FC ports from one or more switches within the same fabric. Port groups are user-specific, you can only view and manage port groups that you create.

The ports display in the order in which you add them to the port group. The order in which you add ports to a port group is persisted in both the port group and the Allow/Prohibit Matrix. While port groups can be at the fabric level (ports from multiple switches within the same fabric), the Allow/Prohibit Matrix is at the switch level. Therefore, when you view the PDCM Allow/Prohibit Matrix for a port group with ports from multiple switches, the matrix only shows the ports for the selected switch.

To reorder the ports you must remove the ports, save your changes, then open the Port Group dialog box and add the ports back to the port group in the new order.

Once you create a port group, you can view and edit the Prohibit Dynamic Connectivity Mask (PDCM) Allow/Prohibit Matrix for the port group. PDCM is a FICON port attribute that can be used to prohibit communication between specific ports. For more information about the PDCM Allow/Prohibit Matrix, refer to [“Configuring a PDCM Allow/Prohibit Matrix”](#) on page 468.

## Creating a port group

**NOTE**  
At least one switch must be reachable to create a port group.

To create a port group, complete the following steps.

1. Select **Configure > Port Groups**.  
The **Port Groups** dialog box displays.

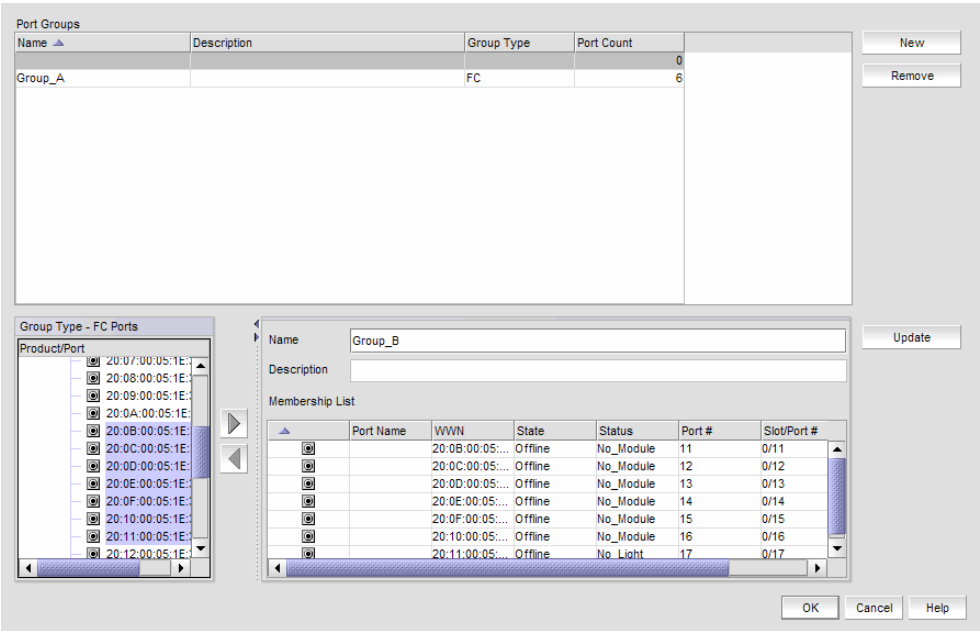


FIGURE 204 Port Groups dialog box

2. Click **New**.
3. Enter a name for the port group in the **Name** field.
4. Enter a description for the port group in the **Description** field.
5. Select one or more ports to add to the group in the **Group Type - FC Ports** table.  
A port group must have at least one port in the **Membership List**. All ports must be from switches in the same fabric.
6. Click the right arrow button.  
The selected ports display in the **Membership List**.
7. Click **Update**.  
The new port group displays in the **Port Groups** table.
8. Click **OK** to close the **Port Groups** dialog box.

### Viewing port groups

Port groups are user-specific, you can only view and manage port groups that you create. To view port groups, complete the following steps.

1. Select **Configure > Port Groups**.

The **Port Groups** dialog box only displays port groups defined by you.

If a fabric becomes un-monitored, any port groups associated with that fabric do not display in the **Port Groups** table. Once the fabric becomes monitored again, the associated port groups display in the **Port Groups** table. For more information about monitoring and un-monitoring fabrics, refer to [“Fabric monitoring”](#) on page 52

If a fabric is removed from discovery, any port groups associated with that fabric are removed permanently from the **Port Groups** dialog box.

If a device is removed from a fabric, then all ports associated with that device are automatically removed permanently from the port group. If the port group only contains ports from the removed device, then the port group is removed permanently from the **Port Groups** dialog box.

If a fabric or device is added to the topology while the **Port Groups** dialog box is open, it does not display in the **Group Type - FC Ports** tree until you close and reopen the **Port Groups** dialog box.

2. Edit the port group, as needed.  
To edit a port group, refer to [“Editing a port group”](#) on page 485.
3. Delete the port group, as needed.  
To delete a port group, refer to [“Deleting a port group”](#) on page 485.
4. Click **OK**.

## Editing a port group

To edit a port group, complete the following steps.

1. Select **Configure > Port Groups**.

The **Port Groups** dialog box displays.

2. Select the port group you want to edit in the **Port Groups** table.

The information for the selected port group displays in the update information area.

3. Change the name for the port group in the **Name** field, if necessary.

---

**NOTE**

If you change the port group name, it is the same as copying the existing port group with a new name.

---

4. Change the description for the port group in the **Description** field, if necessary.

5. Select one or more ports to add to the group in the **Group Type - FC Ports** table.

6. Click the right arrow button.

The selected ports display in the **Membership List**.

7. Select one or more ports to remove from the group in the **Membership List** table.

8. Click the left arrow button.

The selected ports are removed from the **Membership List**.

9. Click **Update**.

10. Click **OK**.

## Deleting a port group

To delete a port group, complete the following steps.

1. Select **Configure > Port Groups**.

The **Port Groups** dialog box displays.

2. Select the port group you want to delete in the **Port Groups** table.

3. Click **Remove**.

The selected ports are removed from the **Port Groups** table.

4. Click **OK**.

## Swapping blades

---

### NOTE

Blade-based port swap is mainly used for FICON and is only applicable for port blades. However, the Management application does not block blade-based port swap for other application blades, including the 8 Gbps 24-port blade.

---

You can swap all of the ports from one blade to another blade. During this operation all ports in the selected blades are swapped. This operation disrupts the traffic on all ports for the selected blades. If GigE ports are present on the blade, only the non-GigE ports are swapped.

To swap blades, you must meet the following requirements:

- The chassis must be running Fabric OS 6.3 or later.
- The chassis must have at least two blades of same type present.

### Example

The source blade has ports sp1 and sp2, and the destination blade has ports dp1 and dp2. During the swap operation, the address sp1 is swapped with dp1 and address sp2 is swapped with dp2.

---

### NOTE

To perform the Swap Blades function you must have Read and Write access for the Product Administration privilege.

---

To swap blades, complete the following steps.

1. Select a chassis that contains at least two of the same type of blades.
  2. Select **Configure > Switch > Swap Blades**.  
The **Swap Blades** dialog box displays.
  3. Select the blade you want to replace from the first **Swap Blades** list.  
Once you select a blade, the second list automatically filters out the selected blade and any blade types that do not match the selected blade.
  4. Select the blade with which you want to replace the first blade from the second **Swap Blades** list.
  5. Select the **Enable ports after swap is complete** check box to enable ports on the destination blade after the swap is complete.
  6. Click **OK**.
- 

### NOTE

This operation disrupts the traffic on all ports for the selected blades.

---

7. Click **Yes** on the confirmation message.

Once the swap blade operation is complete, a 'success' or 'failure' message displays.

# FC-FC Routing Service Management

---

## In this chapter

- [Devices that support Fibre Channel routing . . . . . 487](#)
- [Fibre Channel routing overview . . . . . 488](#)
- [Guidelines for setting up FC-FC routing . . . . . 489](#)
- [Connecting edge fabrics to a backbone fabric . . . . . 490](#)
- [Configuring routing domain IDs . . . . . 492](#)

## Devices that support Fibre Channel routing

The FC-FC Routing Service is supported only on the following devices:

- 40-port, 8 Gbps FC Switch
- 80-port, 8 Gbps FC Switch
- 4 Gbps Router, Extension Switch
- 8 Gbps 16-FC ports, 6-Gbps ports Extension Switch
- Director chassis, when configured with any of the following blades:
  - 4 Gbps Router, Extension Blade
  - FC 8 GB 16-port Blade
  - FC 8 GB 32-port Blade
  - FC 8 GB 48-port Blade - The shared ports area (ports 16-47) cannot be used as EX\_Ports.
  - 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension Blade
- Backbone chassis, when configured with any of the following blades:
  - 4 Gbps Router, Extension Blade
  - FC 8 GB 16-port Blade
  - FC 8 GB 32-port Blade
  - FC 8 GB 48-port Blade - The shared ports area (ports 16-47) cannot be used as EX\_Ports.
  - FC8 GB 64-port Blade
  - 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension Blade

## Fibre Channel routing overview

Fibre Channel routing provides connectivity to devices in different fabrics without merging the fabrics. Using Fibre Channel routing, you can share tape drives across multiple fabrics without the administrative overhead, such as change management and network management, and scalability issues that might result from merging the fabrics.

Fibre Channel routing allows you to create logical storage area networks (LSANs) that can span fabrics. These LSANs allow Fibre Channel zones to cross physical SAN boundaries without merging the fabrics and while maintaining the access controls of zones.

Refer to the *Fabric OS Administrator's Guide* for detailed information about Fibre Channel routing.

The following terminology is used in this chapter:

|                        |                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FC router              | A switch running the FC-FC Routing Service.                                                                                                                                                                                                                                                                                                                                         |
| Interfabric link (IFL) | The link between an E_Port and an EX_Port, or a VE_Port and a VEX_Port.                                                                                                                                                                                                                                                                                                             |
| Edge fabric            | A standard Fibre Channel fabric with targets and initiators connected through an FC router to another Fibre Channel fabric.                                                                                                                                                                                                                                                         |
| Backbone fabric        | The fabric to which the FC router belongs. An FC router connects two or more edge fabrics; a <i>backbone fabric</i> connects FC routers. A backbone fabric consists of at least one FC router and possibly a number of Fabric OS-based Fibre Channel switches. Initiators and targets in the edge fabric can communicate with devices in the backbone fabric through the FC router. |
| LSAN                   | A logical SAN that connects hosts in one fabric with storage devices in another fabric.                                                                                                                                                                                                                                                                                             |
| metaSAN                | The collection of all SANs interconnected with FC routers.                                                                                                                                                                                                                                                                                                                          |

[Figure 205](#) on page 489 shows a metaSAN with a backbone fabric and three edge fabrics. The backbone consists of one 4 Gbps Router, Extension Switch connecting hosts in Edge fabrics 1 and 3 with storage in Edge fabric 2 and the backbone fabric. LSANs provide device sharing between the following pairs of fabrics:

- The backbone fabric and Edge fabric 1
- Edge fabric 1 and Edge fabric 2
- Edge fabric 2 and Edge fabric 3

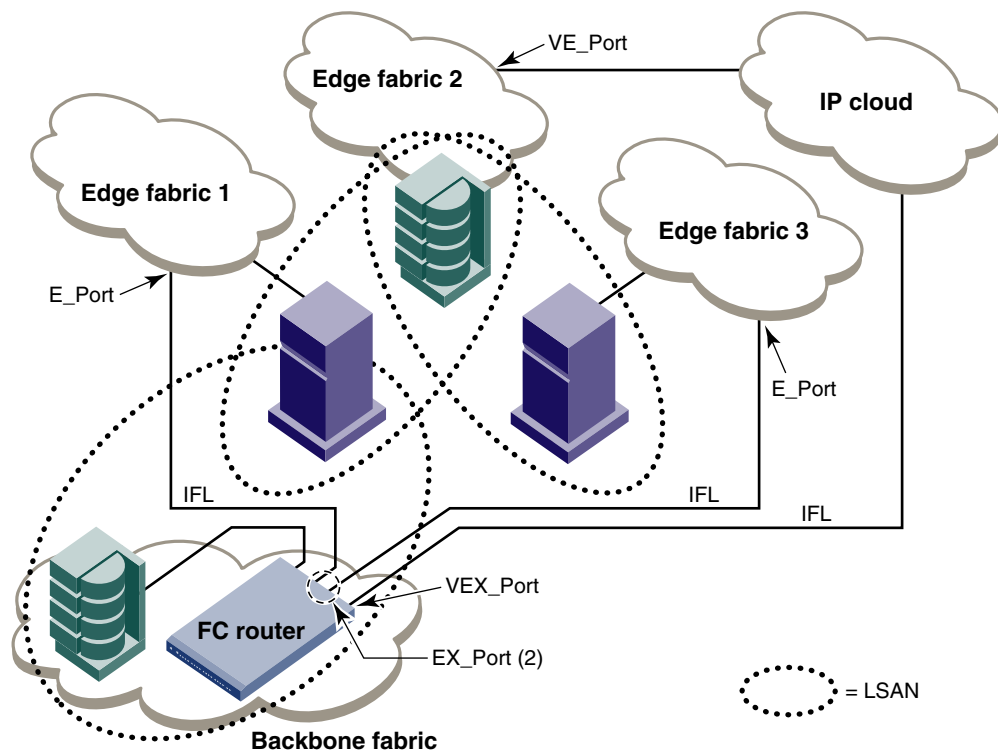


FIGURE 205 A metaSAN with edge-to-edge and backbone fabrics

## Guidelines for setting up FC-FC routing

The following are some general guidelines for setting up FC-FC routing:

- Ensure that the backbone fabric ID of the FC router is the same as that of other FC routers in the backbone fabric.
- On the FC router, ensure that the ports to be configured as EX\_Ports are either disabled or not connected.
- When configuring EX\_Ports, supply a fabric ID for the fabric to which the port will be connected. You can choose any unique fabric ID as long as it is consistent for all EX\_Ports that connect to the same edge fabric.
- For Virtual Fabric (VF)-enabled fabrics, only the base switch can be configured as the FC router; for example, EX\_Ports can be configured only on a base switch for a VF-enabled switch.

# Connecting edge fabrics to a backbone fabric

The following procedure explains how to set up FC-FC routing on two edge fabrics connected through an FC router using E\_Ports and EX\_Ports.

If you are connecting Fibre Channel SANs through an IP-based network, see “[Configuring an FCIP tunnel](#)” on page 391 for instructions on setting up an FCIP tunnel between a VE\_Port and a VEX\_Port.

**ATTENTION**

Be sure that you do not physically connect a port to the remote fabric before configuring it as an EX\_Port; otherwise, the two fabrics merge and you lose the benefit of FC-FC routing.

- 1. Select the edge fabric you want to connect to an FC router from the Connectivity Map or Product List.
- 2. Right-click the edge fabric in the Connectivity Map or Product List and select **Router Configuration**.

The **Router Configuration-Connect Edge Fabric** dialog box is displayed ([Figure 206](#)). The edge fabric you selected is also displayed in the title of the dialog box. Discovered extension switches capable of FC routing are displayed in the **Available Routers** table.

**NOTE**

If the configuration includes virtual fabrics, only the base switch displays in the **Available Routers** table.

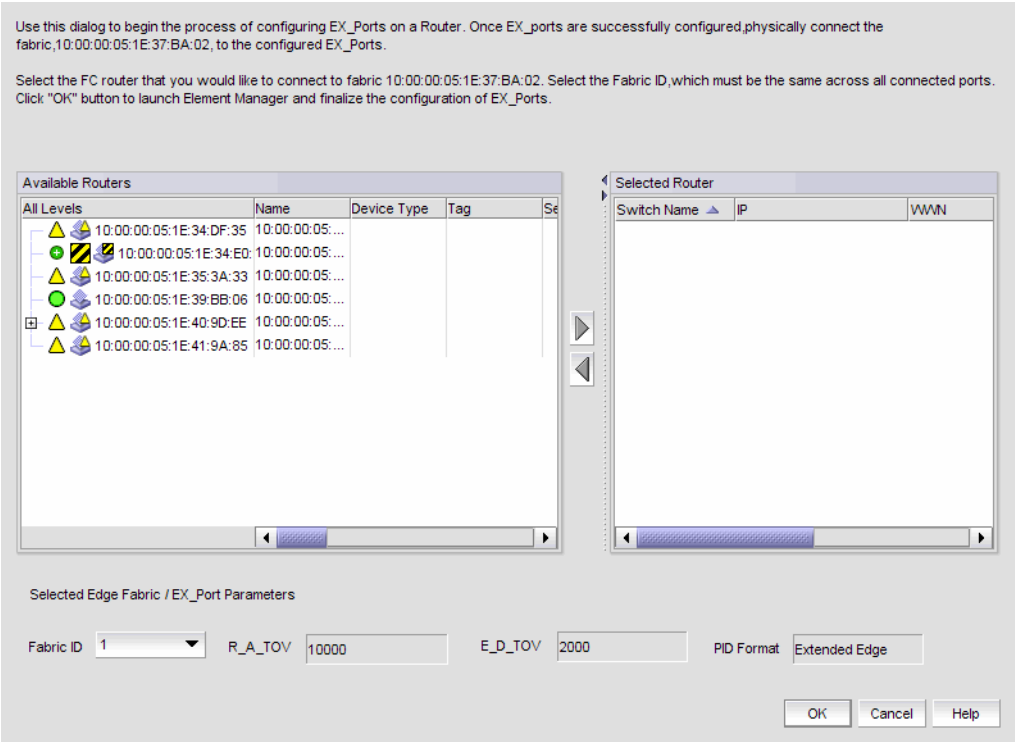


FIGURE 206 Router Configuration-Connect Edge Fabric dialog box

3. Select the FC router from the **Available Routers** table.
4. Click the right arrow to move the FC router you selected to the **Selected Router** table.
5. Select a valid fabric ID (1–128) from the **Fabric ID** list.

You can choose any unique fabric ID as long as it is consistent for all EX\_Ports that connect to the same edge fabric. If the edge fabric is already configured with the backbone fabric, the Fabric ID list is disabled and populated with the pre-selected value.

6. Click **OK** on the **Router Configuration-Connect Edge Fabric** dialog box.

The Element Manager launches automatically and opens the **FC Router** dialog box and Port Configuration wizard. For more information, refer to the *Web Tools Administrator's Guide*.

7. Follow the instructions in the Port Configuration wizard to configure the EX\_Port:
  - a. Select the port to be configured as an EX\_Port.
  - b. Ensure the backbone fabric ID of the switch is the same as that of other FC routers in the backbone fabric. The backbone fabric ID is the fabric ID that was selected in the **Router Configuration-Connect Edge Fabric** dialog box.
  - c. Complete the wizard to configure the EX\_Port.
  - d. Physically connect the EX\_Port to the edge fabric, if it is not already connected.
8. Repeat [step 1](#) through [step 7](#) to connect a second edge fabric to the FC router, if your configuration involves two edge fabrics.
9. Configure LSAN zones in each fabric that will share devices.

For specific instructions, refer to [“Configuring LSAN zoning”](#) on page 628.

## Configuring routing domain IDs

Logical (phantom) domains are created to enable routed fabrics. A logical domain called a front domain is created in edge fabrics for every IFL. A logical domain called a translate (Xlate) domain is created in routed fabrics that share devices.

Use the following procedure to change the domain IDs of these logical domains.

1. Right-click the fabric for which you want to configure phantom domains, and select **Routing Domain IDs**.

The **Configure Routing Domain IDs** dialog box is displayed (Figure 207).

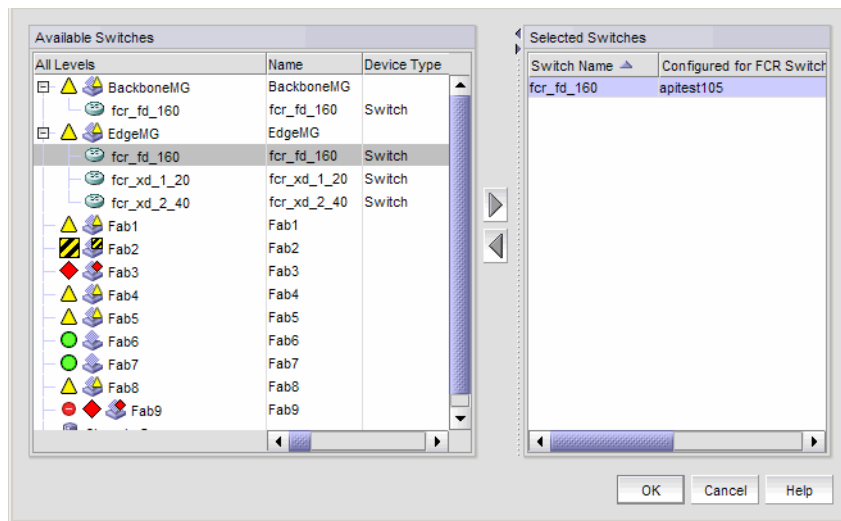


FIGURE 207 Configure Routing Domain IDs dialog box

2. Right-click anywhere in the **Available Switches** table and select **Expand All** to expand the switch group for the fabric to display the FCR logical domains.
3. Select a logical domain, and click the right arrow to move the switch to the **Selected Switches** table.
4. Select a domain ID number from the **Domain ID** list, which lists unused domain IDs.  
You may need to scroll right or drag the dialog box open further to see the **Domain ID** column.
5. Click **OK**.

# Encryption configuration

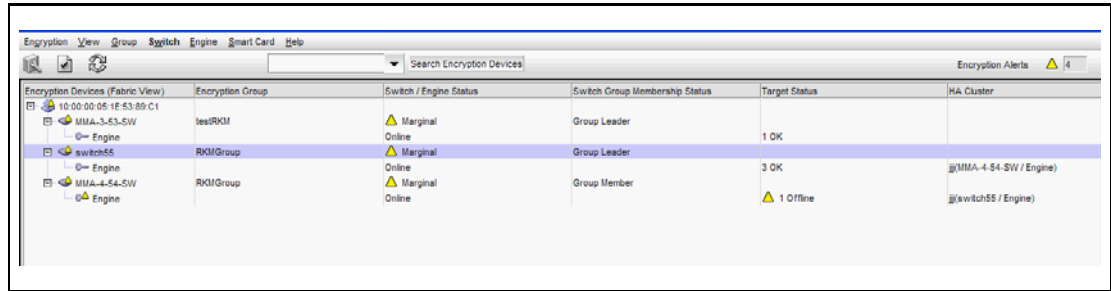
---

## In this chapter

- Encryption Center features ..... 494
- Encryption user privileges ..... 495
- Smart card usage ..... 496
- Network connections ..... 502
- Configuring blade processor links ..... 502
- Encryption node initialization and certificate generation ..... 503
- Supported encryption key manager appliances ..... 504
- Steps for connecting to an RKM appliance ..... 504
- Steps for connecting to an LKM appliance ..... 507
- Steps for connecting to an SKM appliance ..... 511
- Steps for connecting to a TEMS appliance ..... 520
- Gathering information ..... 523
- Creating a new encryption group ..... 524
- Adding a switch to an encryption group ..... 536
- Creating high availability (HA) clusters ..... 541
- Adding encryption targets ..... 544
- Configuring hosts for encryption targets ..... 551
- Adding target disk LUNs for encryption ..... 552
- Adding Target Tape LUNs for encryption ..... 556
- Configuring encrypted tape storage in a multi-path environment ..... 557
- Master keys ..... 559
- Zeroizing an encryption engine ..... 569

## Encryption Center features

The **Encryption Center** dialog box (Figure 208) is the single launching point for all encryption-related configuration in the Management application. It also provides a table that shows the general status of all encryption-related hardware and functions at a glance.



| Encryption Devices (Fabric View)                 | Encryption Group | Switch / Engine Status | Switch Group Membership Status | Target Status | HA Cluster            |
|--------------------------------------------------|------------------|------------------------|--------------------------------|---------------|-----------------------|
| 10:00:00 05:1E:53:89:C1<br>MMA-3-53-SW<br>Engine | testRKM          | Marginal<br>Online     | Group Leader                   | 1 OK          |                       |
| switch55<br>Engine                               | RKMGroup         | Marginal<br>Online     | Group Leader                   | 3 OK          | @MMA-4-54-SW / Engine |
| MMA-4-54-SW<br>Engine                            | RKMGroup         | Marginal<br>Online     | Group Member                   | 1 Offline     | @switch55 / Engine    |

**FIGURE 208** Encryption Center dialog box

Beginning with Fabric OS version 6.4, the Encryption Center is dynamically updated to reflect the latest changes based on any of the following events:

- Encryption group creation or deletion.
- A change in encryption group status.
- Addition or removal of an encryption group member.
- Addition or removal of an encryption engine.
- A change in encryption engine status.

If you are using the Encryption Center for the first time, please read the following topics before you begin to perform encryption operations:

- [“Encryption user privileges”](#) on page 495 describes the Role-based Access Control privileges that are specific to encryption.
- [“Smart card usage”](#) on page 496 and the topics that follow describe the options available for the use of Smart Cards for user authentication, system access control, and storing backup copies of data encryption master keys.
- [“Network connections”](#) on page 502 describes the network connections that must be in place to enable encryption.
- [“Configuring blade processor links”](#) on page 502 describes the steps for interconnecting encryption switches or blades in an encryption group through a dedicated LAN. This must be done before their encryption engines are enabled. Security parameters and certificates cannot be exchanged if these links are not configured and active.
- [“Encryption node initialization and certificate generation”](#) on page 503 lists the security parameters and certificates that are generated when an encryption node is initialized.
- [“Supported encryption key manager appliances”](#) on page 504 lists the supported key manager appliances, and lists topics that provide additional detail.

## Encryption user privileges

In the Management application, resource groups are assigned privileges, roles, and fabrics. Privileges are not directly assigned to users; users get privileges because they belong to a role in a resource group. A user can only belong to one resource group at a time.

The Management application provides three pre-configured roles:

- Storage encryption configuration.
- Storage encryption key operations.
- Storage encryption security.

[Table](#) lists the associated roles and their read/write access to specific operations.

| Privilege                         | Read/Write                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Encryption Configuration  | <p>Enables the following functions from the <b>Encryption Center</b> dialog box:</p> <ul style="list-style-type: none"> <li>• Launch the Configure Encryption dialog.</li> <li>• View switch, group, or engine properties.</li> <li>• View the Encryption Group Properties Security tab.</li> <li>• View encryption targets, hosts, and LUNs.</li> <li>• View LUN centric view</li> <li>• View all re-key sessions</li> <li>• Add/remove paths and edit LUN configuration on LUN centric view</li> <li>• Rebalance encryption engines.</li> <li>• Decommission LUNs</li> <li>• Edit smart card</li> <li>• Create a new encryption group or add a switch to an existing encryption group.</li> <li>• Edit group engine properties (except for the Security tab)</li> <li>• Add targets.</li> <li>• Select encryption targets and LUNs to be encrypted or edit LUN encryption settings.</li> <li>• Edit encryption target hosts configuration.</li> </ul> |
| Storage Encryption Key Operations | <p>Enables the following functions from the <b>Encryption Center</b> dialog box:</p> <ul style="list-style-type: none"> <li>• Launch the Configure Encryption dialog.</li> <li>• View switch, group, or engine properties,</li> <li>• View the Encryption Group Properties Security tab.</li> <li>• View encryption targets, hosts, and LUNs.</li> <li>• Initiate manual LUN re-keying.</li> <li>• Enable and disable an encryption engine.</li> <li>• Zeroize an encryption engine.</li> <li>• Restore a master key.</li> <li>• Edit key vault credentials.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                 |
| Storage Encryption Security       | <p>Enables the following functions from the <b>Encryption Center</b> dialog box:</p> <ul style="list-style-type: none"> <li>• Launch the Configure Encryption dialog.</li> <li>• View switch, group, or engine properties.</li> <li>• View encryption targets, hosts, and LUNs.</li> <li>• Create a master key.</li> <li>• Backup a master key.</li> <li>• View and modify settings on the Encryption Group Properties Security tab (quorum size, authentication cards list and system card requirement).</li> <li>• Establish link keys for LKM key managers.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                               |

## Smart card usage

Smart Cards are credit card-sized cards that contain a CPU and persistent memory. Smart cards can be used as security devices. You must have Storage Encryption Security user privileges to activate, register, and configure smart cards.

Smart cards can be used to do the following:

- Control user access to the Management application security administrator roles.
- Control activation of encryption engines.
- Securely store backup copies of master keys.

Smart card readers provide a plug-and-play interface to read and write to a smart card. The following smart card readers are supported:

- GemPlus GemPC USB  
<http://www.gemalto.com/readers/index.html>
- SCM MicrosystemsSCR331  
[http://www.scmmicro.com/security/view\\_product\\_en.php?PID=2](http://www.scmmicro.com/security/view_product_en.php?PID=2)

See the following procedures for instructions about how to manage smart cards:

- “[Registering authentication cards from a card reader](#)” on page 496
- “[Registering system cards from a card reader](#)” on page 499
- “[Tracking smart cards](#)” on page 500
- “[Saving a master key to a smart card set](#)” on page 563
- “[Restoring a master key from a smart card set](#)” on page 567

### Registering authentication cards from a card reader

When authentication cards are used, one or more authentication cards must be read by a card reader attached to a Management application PC to enable certain security sensitive operations. These include the following:

- Master key generation, backup, and restore operations.
- Replacement of authentication card certificates.
- Enabling and disabling the use of system cards.
- Changing the quorum size for authentication cards.
- Establishing a trusted link with the NetApp LKM key manager.
- Decommissioning LUNs.

To register an authentication card or a set of authentication cards from a card reader, have the cards physically available. Authentication cards can be registered during encryption group or member configuration when running the configuration wizard, or they can be registered using the following procedure.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Select an encryption group, and select **Security Settings**.

3. Select the **Quorum Size**.

The quorum size is the minimum number of cards necessary to enable the card holders to perform the security sensitive operations listed above. The maximum quorum size is five cards. The actual number of authentication cards registered is always more than the quorum size, so if you set the quorum size to five, for example, you will need to register at least six cards in the subsequent steps.

---

**NOTE**

Ignore the **System Cards** setting. Refer to [“Tracking smart cards”](#) on page 500 for information on its usage.

---

4. Click **Next**.

The **Register Authentication Cards** dialog is displayed. This dialog include a table that shows all registered authentication cards.

5. Select **Register from Card Reader** to register a new card.

The **Add Authentication Card** dialog box is displayed.

6. Insert a smart card into the card reader. Be sure to wait for the card serial number to appear, and then enter card assignment information, as directed.

7. Click **OK**.

8. Wait for the confirmation dialog box indicating initialization is done, and click **OK**.

The card is added to the **Registered Authentication Cards** table on the **Authentication Cards** dialog box.

9. Repeat steps 7 through 10 until you have registered all the cards, and they all display in the **Registered Authentication Cards** table on the **Authentication Cards** dialog box. Remember that you need to register the number selected as the quorum size plus one.

## Registering authentication cards from the database

Smart cards that are already in the Management program’s database can be registered as authentication cards.

1. From the **Register Authentication Cards** dialog box, select **Register from Archive**.

The **Authentication Cards** dialog box displays, showing a list of smart cards in the database.

2. Select the card from the table, and click **OK**.

3. Wait for the confirmation dialog box indicating initialization is done, and click **OK**.

The card is added to the **Registered Authentication Cards** table.

## De-registering an authentication card

Authentication cards can be removed from the database and the switch by de-registering them. Use the following procedure to de-register an authentication card.

1. Select the authentication card on the **Authentication Card** table.
2. Click **Deregister**.
3. A confirmation dialog box is displayed. Click **OK** to confirm de-registration.  
The **Encryption Group** dialog box displays.
4. Click **OK** on the **Encryption Group** dialog box.  
The card is de-registered from the group.

## Using authentication cards

When a quorum of authentication cards are registered for use, an **Authenticate** dialog box is displayed to grant access to the following:

- The **Encryption Group Properties** dialog box **Link Keys** tab.
- The **Encryption Group Properties** dialog box **Security** tab, which provides access to the following:
  - **Master Key Actions**, which includes **Backup Master Key**, **Restore Master Key**, and **Create Master Key**.
  - The **System Cards** radio buttons used to specify whether or not a system card is **Required** or **Not Required**.
  - The **Authentication Card Quorum Size** selector.
  - The **Register from Card Reader** and **Register From Archive** buttons.
- The **Master Key Backup** dialog box.
- The **Master Key Restore** dialog box.
- The **Decommission LUNs** dialog box.

To authenticate using a quorum of authentication cards, do the following:

1. When the **Authenticate** dialog box is displayed, gather the number of cards needed, as directed by instructions on the dialog box. The currently registered cards and the assigned owners are listed in the table near the bottom of the dialog box.
2. Insert a card, and wait for the ID to appear in the **Card ID** field.
3. Enter the assigned password.
4. Click **Authenticate**.
5. Wait for the confirmation dialog box, and click **OK**.
6. Repeat steps two through five for each card until the quorum is reached.
7. Click **OK**.

## Enabling or disabling the system card requirement

If you want to use a system card to control activation of an encryption engine on a switch, you must enable the system card requirement. You can use the following procedure to enable or disable the system card requirement.

1. From the **Encryption Center** select an encryption group, and select the **Security** menu.  
The **Select Security Settings** dialog is displayed.
2. Set **System Cards** to **Required** to require the use a system card to control activation of an encryption engine. If **System Cards** is set to **Not Required**, the encryption engine activates without the need to read a system card first.
3. Click **OK**.

## Registering system cards from a card reader

System cards are smart cards that can be used to control activation of encryption engines. Encryption switches and blades have a card reader that enables the use of a system card. System cards discourage theft of encryption switches or blades by requiring the use of a system card at the switch or blade to enable the encryption engine. When the switch or blade is powered off, the encryption engine will not work without first inserting a system card into its card reader. If someone removes a switch or blade with the intent of accessing the encryption engine, it will function as an ordinary FC switch or blade when it is powered up, but use of the encryption engine is denied.

To register a system card from a card reader, a smart card must physically available. System cards can be registered during encryption group creation or member configuration when running the configuration wizard, or they can be registered using the following procedure.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Select the switch from the **Encryption Devices** table, and select **Switch > System Cards** from the menu task bar, or right-click the switch or and select **System Card**.  
The **Register System Card** dialog box is displayed.
3. Insert a smart card into the card reader. Be sure to wait for the card serial number to appear, and then enter card assignment information, as directed.
4. Click **OK**.
5. Wait for the confirmation dialog box indicating initialization is done, and click **OK**.  
The card is added to the **Registered System Cards** table on the **System Cards** dialog box.
6. Store the card in a secure location, not in the proximity of the switch or blade.

De-registering a system card

System cards can be removed from the database by de-registering them. Use the following procedure to de-register a system card.

- 1. From the **Register System Card** dialog box, select the system card you want to de-register.
- 2. Click **Deregister**.
- 3. A confirmation dialog box is displayed. Click **OK** to confirm de-registration.  
The card is removed to the **Registered System Cards** table.

Tracking smart cards

Use the **Smart Card Tracking** dialog box to track smart card details.  
From the **Encryption Center**, select **Smart Card > Smart Card Tracking**.  
The **Smart Card Tracking** dialog box displays (Figure 209).

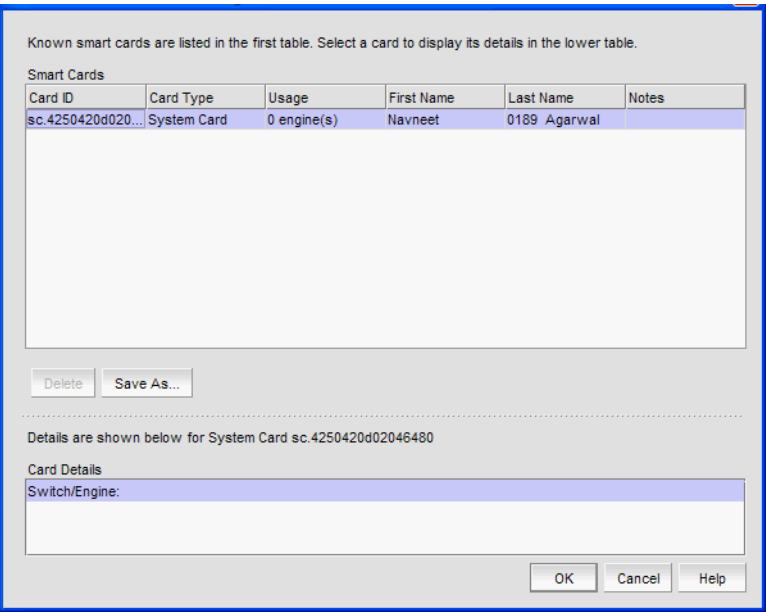


FIGURE 209 Smart Card asset tracking dialog box

Clicking the **Delete** button removes a selected smart card from the Management application database. Deleting smart cards from the Management application database keeps the **Smart Cards** table at a manageable size, but does not invalidate the smart card. The smart card can still be used. You must de-register a smart card to invalidate its use.

**NOTE**  
The **Delete** operation applies only to recovery cards.

Clicking the **Save As** button saves the entire list of smart cards to a file. The available formats are comma-separated values (.csv) and HTML files (.html).

## Editing smart cards

Use the **Edit Smart Card** dialog box to edit smart card details.

1. From the **Encryption Center**, select **Smart Card > Edit Smart Card**.

The **Edit Smart Card** dialog box displays (Figure 210).

To edit a smart card, you will need a card reader attached to the management station.

1) Insert a card into the card reader and wait for the card's ID to appear below. Then enter the card password and click Login button to retrieve card information from the card.

Card ID

Card Password

2) Change card assignment information.

Card Assignment

First Name Last Name

Notes

3) To change the password, select the check box below and enter the new password.

☐ Change password

New Password

Case sensitive, 8-64 characters

Re-type Password

Status: Waiting for card to be inserted ...

**FIGURE 210** Edit Smart Card dialog box

2. Insert the smart card into the card reader.
3. After the card's ID is displayed in the **Card ID** field, enter the **Card Password** and click **Login**.
4. Edit the card assignment user information as needed.
5. Click **OK**.

## Network connections

Before you use the encryption setup wizard for the first time, you must have the following required network connections:

- The management ports on all encryption switches and 384-port Backbone Chassis CPs that have encryption blades installed must have a LAN connection to the SAN management program, and must be available for discovery.
- A supported key management appliance must be connected on the same LAN as the management port of the encryption switches, 384-port Backbone Chassis CPs, and the SAN Management program.
- In some cases, you may want to have an external host available on the LAN to facilitate certificate exchange between encryption nodes and the key management appliance. You may use the SAN management program host computer rather than an external host.
- All switches in the planned encryption group must be interconnected on a private LAN. This LAN is used to exchange security parameters and certificates, and to synchronize encryption engine operations. Refer to [“Configuring blade processor links”](#) on page 502 for details.

## Configuring blade processor links

Each encryption switch or blade has two GbE ports labeled Ge0 and Ge1. The Ge0 and Ge1 ports are Ethernet ports that connect encryption switches and blades to other encryption switches and blades. Both ports of each encryption switch or blade must be connected to the same IP network, and the same subnet. Static IP addresses should be assigned. VLANs should not be used, and DHCP should not be used. These two ports are bonded together as a single virtual network interface to provide link layer redundancy.

All encryption switches or blades in an encryption group must be interconnected by these links through a dedicated LAN before their encryption engines are enabled. Security parameters and certificates cannot be exchanged if these links are not configured and active.

Take the following steps to configure blade processor links.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Right click on the encryption engine, and select **Blade Processor Link**.  
The **Blade Processor Link** dialog box displays.
3. Enter the link IP address and mask, and the gateway IP address.
4. Click **OK**.

The **Blade Processor Link** dialog box may also be launched from the following locations:

- Select **Group > HA Clusters** and select the **Configure Blade Processor Link** button.
- Select a Group, Switch or Encryption Engine, select **Targets > LUN** and select the **Configure Blade Processor Link** button.

## Encryption node initialization and certificate generation

When an encryption node is initialized, the following security parameters and certificates are generated:

- FIPS crypto officer
- FIPS user
- Node CP certificate
- A self-signed Key authentication center (KAC) certificate
- A Key authentication center (KAC) signing request (CSR)

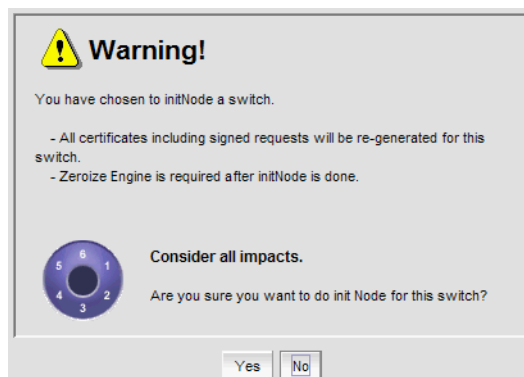
From the standpoint of external SAN management application operations, the FIPS crypto officer, FIPS user, and node CP certificates are transparent to users. The KAC certificates are required for operations with key managers. In most cases, KAC certificate signing requests must be sent to a Certificate Authority (CA) for signing to provide authentication before the certificate can be used. In all cases, signed KACs must be present on each switch.

Encryption nodes are initialized by the **Configure Switch Encryption** wizard when you confirm a configuration.

Encryption nodes may also be initialized from the Encryption Center.

1. From the **Encryption Center**, select **Switch > Init Node**.

The following warning displays.



2. Select **Yes** to initialize the node.

## Supported encryption key manager appliances

As stated under [“Network connections”](#), a supported key management appliance must be connected on the same LAN as the management port of the encryption switches or of the Backbone Chassis Control Processors (CPs) in the case of the encryption blade.

Secure communication between encryption nodes in an encryption group, and between encryption nodes and key manager appliances requires an exchange of certificates that are used for mutual authentication. Each supported key manager appliance has unique requirements for setting up a secure connection and exchanging certificates.

The following key manager appliance are supported:

- The RSA Key Manager (RKM)
- The NetApp Lifetime Key Manager (LKM)
- The HP StorageWorks Secure Key Manager (SKM)
- The Thales Encryption Manager for Storage (TEMS)

Refer to the following topics for specific information:

- [“Steps for connecting to an RKM appliance”](#) on page 504.
- [“Steps for connecting to an LKM appliance”](#) on page 507.
- [“Steps for connecting to an SKM appliance”](#) on page 511.
- [“Steps for connecting to a TEMS appliance”](#) on page 520.

## Steps for connecting to an RKM appliance

All switches you plan to include in an encryption group must have a secure connection to the RSA Key Manager (RKM). The following is a suggested order for the steps needed to create a secure connection to RKM:

3. Export the KAC CSR to a location accessible to a Certificate Authority (CA) for signing.
4. Submit the KAC CSR for signing by a Certificate Authority (CA).
5. Import the signed certificate into the Brocade encryption node.
6. Upload the signed KAC and CA certificates onto the RKM appliance, and select the appropriate key classes.
7. If dual RKM appliances are used for high availability, the RKM appliances must be clustered, and must operate in maximum availability mode, as described in the RKM appliance user documentation.

These steps are described in more detail in the following sections.

## Exporting the KAC certificate signing request (CSR)

You need to export the KAC CSR to a temporary location prior to submitting the KAC CSR to a Certificate Authority (CA) for signing.

1. Synchronize the time on the switch and the key manager appliance. They should be within one minute of each other. Differences in time can invalidate certificates and cause key vault operations to fail.
2. From the **Encryption Center**, right-click on the switch and select **Properties**.
3. If a CSR is present, click **Export**. If a CSR is not present, right-click on the switch and select **Initnode**. This generates switch security parameters and certificates, including the KAC CSR.

A dialog box displays.

- 4.
5. Select Yes to store the file. The default location for the exported file is **My Documents**.

---

### NOTE

The CSR is exported in Privacy Enhanced Mail (.pem) format. This is the format required in exchanges with certificate authorities.

---

## Submitting the CSR to a certificate authority

The CSR must be submitted to a certificate authority (CA) to be signed. The certificate authority is a trusted third party entity that signs the CSR. There are several CAs available, and procedures vary, but the general steps are as follows.

1. Open an SSL connection to an X.509 server.
2. Submit the CSR for signing.
3. Request the signed certificate.

Generally, a public key, the signed KAC certificate, and a signed CA certificate are returned.

4. Download and store the signed certificates.

The following example submits a CSR to the demoCA from RSA.

```
cd /opt/CA/demoCA
openssl x509 -req -sha1 -CAcreateserial -in certs/KACcsr kac_RKM_cert.pem
-days 365 -CA ca
```

## Importing the signed KAC certificate

After a KAC CSR has been submitted and signed by a CA, the signed certificate must be imported into the switch.

1. From the Encryption Center, select **Switch > Import Certificate**.  
The **Import Signed Certificate** dialog box displays.
2. Browse to the location where the signed certificate is stored.
3. Click **OK**.

The signed certificate is stored on the switch.

## Uploading the KAC and CA certificates onto the RKM appliance

After an encryption group is created, you need to install the switch public key certificate (KAC certificate) and signing authority certificate (CA certificate) on the RKM appliance.

1. Start a web browser, and connect to the RKM appliance setup page. You will need the URL, and have the proper authority level, a user name, and a password.
2. Select the **Operations** tab.
3. Select **Certificate Upload**.
4. In the **SSLCertificateFile** field, enter the full local path of the CA certificate. Do not use the UNC naming convention format.
5. Select **Upload, Configure SSL**, and **Restart Webserver**.
6. After the web server restarts, enter the root password.
7. Open another web browser window, and start the RSA management user interface.  
You will need the URL, and have the proper authority level, a user name, and a password.

---

### NOTE

The Identity Group name used in the next step may not exist in a freshly installed RKM. To establish an Identity Group name, click the **Identity Group** tab, and create a name. The name **Hardware Retail Group** is used as an example in the following steps.

---

8. Select the **Key Classes** tab. For each of the following key classes, perform steps a. through h. to create the class. The key classes must be created only once, regardless of the number of nodes in your encryption group and regardless of the number of encryption groups that will be sharing this RKM.
  - `kcn.1998-01.com.brocade:DEK_AES_256_XTS`
  - `kcn.1998-01.com.brocade:DEK_AES_256_CCM`
  - `kcn.1998-01.com.brocade:DEK_AES_256_GCM`
  - `kcn.1998-01.com.brocade:DEK_AES_256_ECB`
  - a. Click **Create**.
  - b. Type the key name string into the **Name** field.
  - c. Select **Hardware Retail Group** for **Identity Group**.
  - d. Deselect **Activated Keys Have Duration**.
  - e. Select **AES** for **Algorithm**.
  - f. Select **256** for **Key Size**.
  - g. Select the **Mode** for the respective key classes as follows:
    - XTS** for Key Class "kcn.1998-01.com.brocade:DEK\_AES\_256\_XTS"
    - CBC** for Key Class "kcn.1998-01.com.brocade:DEK\_AES\_256\_CCM"
    - CBC** for Key Class "kcn.1998-01.com.brocade:DEK\_AES\_256\_GCM"
    - ECB** for Key Class "kcn.1998-01.com.brocade:DEK\_AES\_256\_ECB"
  - h. Click **Next**.

- i. Repeat a. through h. for each key class.
  - j. Click **Finish**.
9. For each encryption node, create an identity as follows.
  - a. Select the **Identities** tab.
  - b. Click **Create**.
  - c. Enter a label for the node in the **Name** field. This is a user-defined identifier.
  - d. Select the **Hardware Retail Group** in the **Identity Groups** field.
  - e. Select the **Operational User** role in the **Authorization** field.
  - f. Click **Browse** and select the imported certificate as the **Identity certificate**.
  - g. Click **Save**.

## RKM key vault high availability deployment

When dual RKM appliances are used for high availability, the RKM appliances must be clustered, and must operate in maximum availability mode, as described in the RKM appliance user documentation.

When dual RKM appliances are clustered, they are accessed using an IP load balancer. For a complete high availability deployment, the multiple IP load balancers are clustered, and the IP load balancer cluster exposes a virtual IP address called a floating IP address. The floating IP address must be registered on the Brocade encryption group leader.

The secondary RKM appliance must not be registered, and also individual RKM appliance IP addresses must not be registered.

## Steps for connecting to an LKM appliance

The NetApp Lifetime Key Manager (LKM) resides on an FIPS 140-2 Level 3-compliant network appliance. The encryption engine and LKM appliance communicate over a trusted link. A trusted link is a secure connection established between the Encryption switch or blade and the NetApp LKM appliance, using a shared secret called a link key.

The following configuration steps are performed from the NetApp DataFort Management Console and from the Management application:

- Install and launch the NetApp DataFort Management Console.
- Establish the trusted link.
- Obtain and import the LKM certificate.
- Export and register encryption node certificates on LKM.
- If required, create an LKM cluster for high availability.

These steps are described in more detail in the following sections.

## The NetApp DataFort Management Console

The NetApp DataFort Management Console (DMC) must be installed on your PC or workstation to complete certain procedures described in this appendix. Refer to the appropriate DMC product documentation for DMC installation instructions. After you install DMC, do the following.

1. Launch the DMC.
2. Click the **Appliance** tab on the top panel.
3. Add the NetApp LKM appliance IP address or hostname.
4. Right-click the added IP address and log into the NetApp LKM key vault.

## Establishing the trusted link

You must generate the trusted link establishment package (TEP) on all nodes to obtain a trusted acceptance package (TAP) before you can establish a trusted link between each node and the NetApp LKM appliance.

1. From the **Encryption Center**, select **Group > Link Keys**.  
The switch name displays in the link status table under **Switch**, with a **Link Key Status** of **Link Key requested, pending LKM approval**.
2. Select the switch, and click **Establish**.  
This results in a Trusted link establishment package (TEP), which is needed to establish the trusted link between the switch and the LKM appliance.
3. Launch the NetApp DataFort Management Console (DMC) and click the **View Unapproved Trustees** tab.  
The switch is listed as openkey\_trustee\_<ip address>, where the IP address is the switch IP address.
4. Select the switch, and click **Approve and Create TAP**.  
The **Approve TEP** dialog box displays. The TEP must be approved before a TAP can be created.
5. Provide a label in the dialog box and click **Approve** to approve the TEP.  
A list of recovery cards and recovery officers is displayed. TEP approval is done by a quorum of recovery officers, using assigned recovery cards. Each recovery officer must individually insert one of listed recovery cards into a card reader attached to the PC or workstation, enter the password for that card, and click **Start**. The procedure is repeated until a quorum of recovery officers has approved the TEP.
6. Save the TAP to a file (location does not matter).
7. Select the **Link Keys** tab on the **Encryption Group Properties** dialog box.
8. Select the switch in the link key status table, and click **Accept** to retrieve the TAP from the LKM appliance.
9. Repeat the above steps for each of the remaining member nodes.

## Obtaining and importing the LKM certificate

Certificates must be exchanged between LKM and the encryption switch to enable mutual authentication. You must obtain a certificate from LKM, and import it into the encryption group leader. The encryption group leader exports the certificate to other encryption group members.

To obtain and import an LKM certificate, do the following.

1. Open an SSH connection to the NetApp LKM appliance and log in.

```
host$ssh admin@10.33.54.231
admin@10.33.54.231's password:

Copyright (c) 2001-2009 NetApp, Inc.
All rights reserved
+-----+
| NetApp Appliance Management CLI |
|           Authorized use only!   |
+-----+
Cannot read termcapdatabase;
using dumb terminal settings.
Checking system tamper status:
No physical intrusion detected.
```

2. Add the group leader to the LKM key sharing group. Enter **lkmserver add --type third-party --key-sharing-group "/"** followed by the group leader IP address.

```
lkm-1>lkmserver add --type third-party --key-sharing-group \
"/" 10.32.244.71
NOTICE: LKM Server third-party 10.32.244.71 added.
Cleartext connections not allowed.
```

3. On the NetApp LKM appliance terminal, enter **sys cert getcert-v2** to display the LKM certificate content.

```
lkm-1> sys cert getcert-v2
-----BEGIN CERTIFICATE-----
[content removed]
-----END CERTIFICATE-----
```

4. Copy and paste the LKM certificate content from the NetApp LKM appliance terminal into an editor buffer. Save the file as **lkmcert.pem** on the SCP-capable host. Save the entire certificate, including the lines **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----**.
5. If you are using DCFM, the path to the file must be specified on the **Select Key Vault** dialog box when creating a group leader. If the proper path is entered, the file is imported.

## Exporting and registering the switch KAC certificates on LKM

The encryption switch self-signed KAC certificates must be exported and then registered on the LKM appliance.

1. From the **Encryption Center**, select **Switch > Export Certificate**.

The **Export Switch Certificate** dialog box displays.

2. Select **Self-signed switch certificate (X.509)** and click **OK**.

A dialog box displays that allows you to save the CSR to your SAN Management Program client PC, or an external host of your choosing.

3. Register the self-signed KAC certificate you exported from the member node with the NetApp LKM appliance.

## LKM key vault high availability deployment

LKM appliances can be clustered together to provide high availability capabilities. You can deploy and register one LKM with an encryption switch or blade and later deploy and register another LKM at any time, if LKMs are clustered or linked together. Please refer to LKM documentation to link or cluster the LKMs.

When LKM appliances are clustered, both LKMs in the cluster must be registered and configured with the link keys before starting any crypto operations. If two LKM key vaults are configured, they must be clustered. If only a single LKM key vault is configured, it may be clustered for backup purposes, but it will not be directly used by the switch.

When dual LKMs are used with the encryption switch or blade, the dual LKMs must be clustered. There is no enforcement done at the encryption switch or blade to verify whether or not the dual LKMs are clustered, but key creation operations will fail if you register non-clustered dual LKMs with the encryption switch or blade.

Regardless of whether you deploy a single LKM or clustered dual LKMs, register only the primary key vault with the encryption switch or blade. You do not need to register a secondary key vault.

## Disk keys and tape pool keys (Brocade native mode support)

DEK creation, retrieval, and update for disk and tape pool keys in Brocade native mode are as follows:

- **DEK creation** - The DEK is archived into the primary LKM. Upon successful archive of DEK onto primary LKM, the DEK is read from secondary LKM until it is synchronized to the secondary LKM, or a timeout of 10 seconds occurs (2 seconds with 5 retries). If successful, then the DEK created can be used for encrypting disk LUNs or tape pool in Brocade native mode. If key archival of the DEK to primary LKM fails, an error is logged and the operation is retried. If the failure happens after archival of the DEK to the primary LKM, but before synchronization to the secondary, a VAULT\_OFFLINE error is logged and the operation is retried. Any DEK archived to the primary in this case is not used.
- **DEK retrieval** - The DEK is retrieved from the primary LKM if the primary LKM is online and reachable. If the registered primary LKM is not online or not reachable, the DEK is retrieved from a clustered secondary LKM.
- **DEK Update** - DEK Update behavior is same as DEK Creation.

## Tape LUN and DF -compatible tape pool support

- **DEK Creation** - The DEK is created and archived to the primary LKM only. Upon successful archival of the DEK to the primary LKM, the DEK can be used for encryption of a Tape LUN or DF-Compatible tape pool. The DEK is synchronized to a secondary LKM through LKM clustering. If DEK archival to the primary LKM fails, DEK archival is retried to the clustered secondary LKM. If DEK archival also fails to secondary LKM, an error is logged and the operation is retried.
- **DEK retrieval** - The DEK is retrieved from primary LKM if primary is online and reachable. If primary LKM is not online or not reachable, the DEK is retrieved from the clustered secondary LKM.
- **DEK update** - DEK update behavior is same as DEK Creation.

## LKM Key Vault Deregistration

Deregistration of either Primary or Secondary LKM KV from an encryption switch or blade is allowed independently.

- **Deregistration of Primary LKM** - You can deregister the Primary LKM from an encryption switch or blade without deregistering the backup or secondary LKM for maintenance or replacement purposes. However, when the primary LKM is deregistered, key creation operations will fail until either primary LKM is reregistered or the secondary LKM is deregistered and reregistered as Primary LKM.

When the Primary LKM is replaced with a different LKM, you must first synchronize the DEKs from secondary LKM before reregistering the primary LKM.

- **Deregistration of Secondary LKM** - You can deregister the Secondary LKM independently. Future key operations will use only the Primary LKM until the secondary LKM is reregistered on the encryption switch or blade.

When the Secondary LKM is replaced with a different LKM, you must first synchronize the DEKs from Primary LKM before reregistering the secondary LKM.

## Steps for connecting to an SKM appliance

The SKM management web console can be accessed from any web browser with Internet access to the SKM appliance. The URL for the appliance is as follows:

```
https://<appliance hostname>:<appliance port number>
```

Where:

- <appliance hostname> is the hostname or IP address when installing the SKM appliance.
- <appliance port number> is 9443 by default. If a different port number was specified when installing the SKM appliance, use that port number.

The following configuration steps are performed from the SKM management web console and from the Management application.

- Configure a Brocade group on SKM.
- Register the Brocade group user name and password on the encryption node.
- Set up a local Certificate Signing Authority (CA) on SKM.

- Download the CA certificate.
- Create and install an SKM server certificate.
- Enable an SSL connection.
- Configure a cluster of SKM appliances for high availability.
- Export and sign the encryption node certificate signing requests.
- Import the signed certificates into the encryption node.

These steps are described in more detail in the following sections.

### Configuring a Brocade group on SKM

A Brocade group is configured on SKM for all keys created by Brocade encryption switches and blades. This needs to be done only once for each key vault.

1. Login to the SKM management web console using the admin password.
2. Select the **Security** tab.
3. Select **Local Users & Groups** under **Users and Groups**.  
The **User & Group Configuration** page displays.
4. Select **Add** under **Local Users**.
5. Create a Brocade user name and password.
6. Select the **User Administration Permission** and **Change Password Permission** check boxes.
7. Select **Save** to save this user data.
8. Select **Add** under **Local Groups**.
9. Add a Brocade group under **Group**.
10. Select **Save**.
11. Select the new Brocade group name, and then select **Properties**.  
Local **Group Properties** and a **User List** are displayed.
12. In the **User List** section, select or type the Brocade user name under **Username**.
13. Select **Save**.

The Brocade user name and password are now configured on SKM.

---

#### NOTE

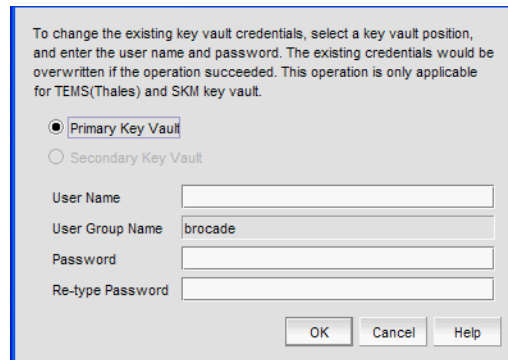
Fabric OS version 6.2.0 uses brcduser1 as a standard user name when creating a Brocade group on SKM. If you downgrade to version 6.2.0, the user name is overwritten to brcduser1, and the Brocade group user name must be changed to brcduser1.

---

## Registering the SKM Brocade group user name and password

The Brocade group user name and password you created when configuring a Brocade group on SKM must also be registered on each Brocade encryption node.

1. From the Encryption Center, select Key Vault Credentials.



2. Enter the Brocade group user name and password.

Keep the following rules in mind when registering the Brocade user name and password:

- The user name and password must match the user name and password specified for the Brocade group.
- The same user name and password must be configured on all nodes in an encryption group. This is not enforced or validated by the encryption group members, so care must be taken when configuring the user name and password to ensure they are the same on each node.
- Different user names and passwords can never be used within the same encryption group, but each encryption group may have its own user name and password.
- If you change the user name and password, the keys created by the previous user become inaccessible. The Brocade group user name and password must also be changed to the same values on SKM to make the keys accessible.
- When storage is moved from one encryption group to another, and the new encryption group uses different user name and password, the Brocade group user name and password must also be changed to the same values on SKM to make the keys accessible.

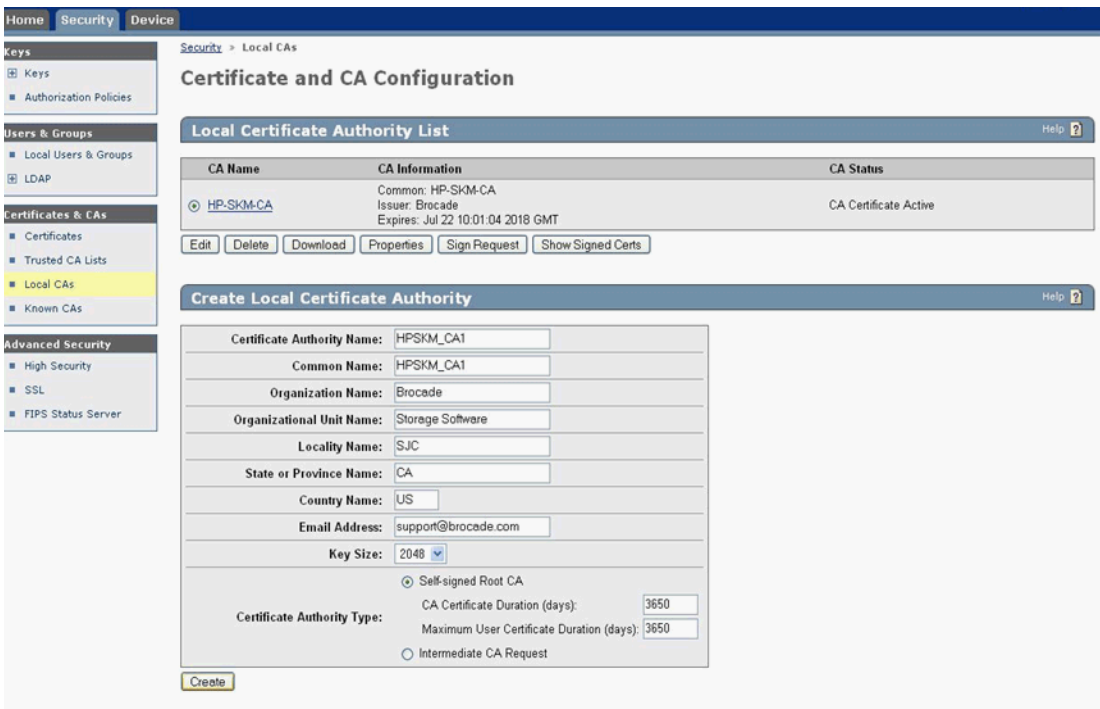
3. Repeat the procedure for each node.

## Setting up the local Certificate Authority (CA) on SKM

To create and install a local CA, perform the following steps:

1. Login to the SKM management web console using the admin password.
2. Select the **Security** tab.
3. Under **Certificates & CAs**, click **Local CAs**.
4. Enter information required by the **Create Local Certificate Authority** section of the window to create your local CA.
  - Enter a **Certificate Authority Name** and **Common Name**. These may be the same value.
  - Enter your organizational information.
  - Enter the **Email Address** to receive messages for the Security Officer.
  - Enter the **Key Size**. HP recommends using 2048 for maximum security.
  - Select **Self-signed Root CA**.
  - Enter the **CA Certification Duration** and **Maximum User Certificate Duration**. These values determine when the certificate must be renewed and should be set in accordance with your company's security policies. The default value for both is 3650 days or 10 years.
5. Click **Create**.

The new local CA displays under **Local Certificate Authority List** (Figure 211).



**FIGURE 211** Creating an HP SKM Local CA

5. Under **Certificates & CAs**, select **Trusted CA Lists** to display the **Trusted Certificate Authority List Profiles**.
6. Click on **Default** under **Profile Name**.

7. In the **Trusted Certificate Authority List**, click **Edit**.
  8. From the list of **Available CAs** in the right panel, select the CA you just created.
- Repeat these steps any time another local CA is needed.

## Downloading the local CA certificate from SKM

The local CA certificate you created using the procedure for [“Setting up the local Certificate Authority \(CA\) on SKM”](#) on page 514 must be saved to your local system. Later, this certificate must be imported onto the Brocade encryption group leader nodes.

1. From the **Security** tab, select **Local CAs** under **Certificates and CAs**.
2. Select the CA certificate you created.
3. Click **Download**, and save the certificate file on your local system.
4. Rename the downloaded file, changing the .cert extension to a .pem extension.

## Creating and installing the SKM server certificate

To create the SKM server certificate, perform the following steps:

1. Click the **Security** tab.
2. Under **Certificates and CAs**, select **Certificates**.
3. Enter the required information under **Create Certificate Request**.
  - Enter a **Certificate Name** and **Common Name**. The same name may be used for both.
  - Enter your organizational information.
  - Enter the **E-mail Address** where you want messages to the Security Officer to go.
  - Enter the **Key Size**. HP recommends using the default value: 1024.

4. Click **Create Certificate Request**.

Successful completion is indicated when the new entry for the server certificate appears on the **Certificate List** with a **Certificate Status** of **Request Pending**.

5. Select the newly created server certificate from the **Certificate List**.
6. Select **Properties**.

The pending request displays under **Certificate Request Information**.

7. Copy the certificate data from -----BEGIN CERTIFICATE REQUEST----- to -----END CERTIFICATE REQUEST----- lines. Be careful to exclude extra carriage returns or spaces after the data.
8. Under **Certificates & CAs**, select **Local CAs**.

The **Certificate and CA Configuration** page is displayed.

9. From the **CA Name** column, select the name of the local CA you just created in [“Setting up the local Certificate Authority \(CA\) on SKM”](#) on page 514.
10. Click **Sign Request**.

11. Enter the required data in the **Sign Certificate Request** section of the window.
  - Select the CA name from the **Sign with Certificate Authority** drop down box.
  - Select **Server** as the **Certificate Purpose**.
  - Enter the number of days before the certificate must be renewed based on your site's security policies. The default value is 3649 or 10 years.
12. Paste the copied certificate request data into the **Certificate Request** box.
13. Click **Sign Request**.

The signed certificate request data displays under **Sign Certificate Request**.
14. Click **Download** to download the signed certificate to your local system.
15. Copy the signed certificate data, from -----BEGIN to END----- lines. Be careful to exclude extra carriage returns or spaces after the data.
16. From the **Security** tab select **Certificates** under **Certificates & CAs**.
17. Select the server certificate name you just created from the certificate list, and select **Properties**.

The **Certificate Request Information** window displays.
18. Click **Install Certificate**.

The **Certificate Installation** window displays.
19. Paste the signed certificate data you copied under **Certificate Response** and click **Save**.

The status of the server certificate should change from **Request Pending** to **Active**.

## Enabling SSL on the Key Management System (KMS) Server

The KMS Server provides the interface to the client. Secure Sockets Layer (SSL) must be enabled on the KMS Server before this interface will operate. After SSL is enabled on the first appliance it will be automatically enabled on the other cluster members.

To configure and enable SSL, perform the following steps:

1. Select the **Device** tab.
2. In the **Device Configuration** menu, click **KMS Server** to display the **Key Management Services Configuration** window.
3. In the **KMS Server Settings** section of the window, click **Edit**. The following warning may display.
4. Configure the KMS Server Settings. Ensure that the port and connection timeout settings are 9000 and 3600, respectively. For **Server Certificate**, select the name of the certificate you created in [“Creating and installing the SKM server certificate”](#) on page 515.
5. Click **Save**.

## Creating an SKM High Availability cluster

The HP SKM key vault supports clustering of HP SKM appliances for high availability. If two SKM key vaults are configured, they must be clustered. If only a single SKM appliance is configured, it may be clustered for backup purposes, but the backup appliance will not be directly used by the switch. The procedures in this section will establish a cluster configuration on one SKM appliance and then transfer that configuration to the remaining appliances.

- Create the cluster on one SKM appliance that is to be a member of the cluster.
- Copy the local CA certificate from the first SKM appliance or an existing cluster member.
- Paste the local CA certificate it into the management console for each of the SKM appliances added to the cluster.

To create a cluster, perform the following steps on one of the HP SKM appliances that is to be a member of the cluster.

1. From the SKM management console, click the **Device** tab.
2. In the **Device Configuration** menu, click **Cluster**.  
The **Create Cluster** section displays.
3. Select and note the **Local IP** address. You will need this address when you add an appliance to the cluster.
4. For **Local Port**, use the default value of 9001 unless you are explicitly directed to use a different value for your site.
5. Type the cluster password in the **Create Cluster** section of the main window to create the new cluster.
6. Click the **Create** button.
7. In the **Cluster Settings** section of the window, click **Download Cluster Key** and save the key to a convenient location, such as your computer's desktop. The cluster key is a text file and is only required temporarily. It may be deleted from your computer's desktop after all SKM appliances have been added to the cluster.

## Copying the local CA certificate for a clustered SKM appliance

Before adding an SKM appliance to a cluster, you must obtain the local CA certificate from the original SKM or from an SKM that is already in the cluster.

1. Select the **Security** tab.
2. Select **Local CAs** under **Certificates & CAs**.
3. Select the name of the local CA from the **Local Certificate Authority** list.

The **CA Certificate Information** is displayed.

4. Copy the certificate request, beginning with `---BEGIN CERTIFICATE REQUEST---` and ending with `---END CERTIFICATE REQUEST---`. Be careful not to include any extra characters.

## Adding SKM appliances to the cluster

If you are adding an appliance to an existing cluster, select the Cluster Settings section of the window, click Download Cluster Key and save the key to a convenient location, such as your computer's desktop.

To add SKM appliances to the cluster you are creating, you will need the original cluster member's local IP address, local port number, and the location of the cluster key you downloaded, as specified in [“Creating an SKM High Availability cluster”](#) on page 517.

Perform the following steps on each SKM appliance you want to add to the cluster.

1. Open a new browser window, keeping the browser window from **Copying the Local CA certificate** open.
2. In the new browser window, log into the management console of the SKM appliance that is being added to the cluster and click the **Security** tab.
3. In the **Certificates & CAs** menu, click **Known CAs**.

Enter information required in the Install CA Certificate section near the bottom of the page.

- Type the **Certificate Name** of the certificate being transferred from the first cluster member.
  - Paste the copied certificate data into the **Certificate** box.
4. Click **Install**.
  5. In the **Certificates & CA** menu, click **Trusted CA Lists**.
  6. Click on the **Default Profile Name**.
  7. Click **Edit**.
  8. Select the name of the CA from the list of **Available CAs** in the right panel.
  9. Click **Add**.
  10. Click **Save**.
  11. Select the **Device** tab.
  12. In the **Device Configuration** menu, click on **Cluster**.
  13. Click on **Join Cluster**. In the **Join Cluster** section of the window, leave **Local IP** and **Local Port** set to their defaults.
  14. Type the original cluster member's local IP address into **Cluster Member IP**.
  15. Type the original cluster member's local Port into **Cluster Member Port**.
  16. Click **Browse** and select the **Cluster Key File** you saved.
  17. Type the cluster password into **Cluster Password**.
  18. Click **Join**.
  19. After adding all members to the cluster, delete the cluster key file from the desktop.
  20. Create and install an SKM server certificate. Refer to [“Creating and installing the SKM server certificate”](#) on page 515 for a description of this procedure.

## Signing the Brocade encryption node KAC certificates

The KAC certificate signing request generated when the encryption node is initialized must be exported for each encryption node and signed by the Brocade local CA on SKM. The signed certificate must then be imported back into the encryption node.

1. From the Encryption Center, select **Switch > Export Certificate**.

The **Export Switch Certificate** dialog box displays.

2. Select **Public Key Certificate Request (CSR)** and click **OK**.

A dialog box displays that allows you to save the CSR to your SAN Management Program client PC.

Alternatively, you may select **Switch > Properties**, and click the **Export** button beside the **Public Key Certificate Request**, or copy the CSR for pasting into the **Certificate Request Copy** area on the SKM **Sign Certificate Request** page.

3. Launch the SKM administration console in a web browser and log in.

4. Select the **Security** tab.

5. Select **Local CAs** under **Certificates & CAs**.

The **Certificate and CA Configuration** page displays.

6. Under **Local Certificate Authority List**, select the Brocade CA name.

7. Select **Sign Request**.

The **Sign Certificate Request** page is displayed.

8. Select **Sign with Certificate Authority** using the Brocade CA name with the maximum of 3649 days option.

9. Select **Client** as **Certificate Purpose**.

10. Allow Certificate **Duration** to default to 3649.

11. Paste the file contents that you copied in step 3 in the **Certificate Request Copy** area.

12. Select **Sign Request**.

Upon success, you are presented with the option of downloading the signed certificate.

13. Download the signed certificate to your local system as signed\_kac\_skm\_cert.pem.

This file is then ready to be imported to the encryption switch or blade.

## Importing a signed KAC certificate into a switch

After a KAC CSR has been submitted and signed by a CA, the signed certificate must be imported into the switch.

1. From the **Encryption Center**, select **Switch > Import Certificate**.

The **Import Signed Certificate** dialog box displays.

2. Browse to the location where the signed certificate is stored.

3. Click **OK**.

The signed certificate is stored on the switch.

## Steps for connecting to a TEMS appliance

TEMS provides a web user interface for management of clients, keys, admins, and configuration parameters. A Thales officer creates domains, groups, and managers (a type of administrator), assigns groups to domains and assigns managers to manage groups. Managers are responsible for creating clients and passwords for the groups they manage.

The following configuration steps are performed from the TEMS web user interface and from the Management application:

- Set up network connections to TEMS.
- Create a TEMS client.
- Establish TEMS key vault credentials.
- Sign encryption node certificate signing requests
- Import the signed requests onto the encryption nodes.

These steps are described in more detail in the following sections.

### Setting up TEMS network connections

Communicating to TEMS is enabled over an SSL connection. Two IP addresses are needed. One IP address is used for the management interface, and a second IP address is used for communications with clients. These IP addresses are typically assigned during the initial set up of the TEMS appliance.

1. Log in to the Thales management program as admin and select the **Network** tab ([Figure 212](#)).

**FIGURE 212** TEMS Network Settings

2. Enter the management IP address information under **Management Interface**.

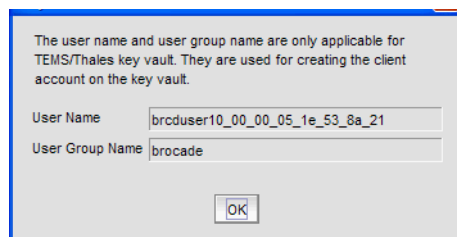
3. Enter the client IP address information under **KM Server Interface**.
4. Enter a host name for the appliance, internet or intranet domain, and, if used, the primary and secondary DNS IP address under **Common Settings**.
5. Set **Service Settings** as shown in [Figure 212](#).
  - HTTPS Port 433
  - SSH Port 22
  - Enable SSH
  - KM Server Port 9000
  - Enable KM Server

## Creating a client on TEMS

This step assumes that the group **brocade** has been created by an administrator. If the group **brocade** does not exist, you must log in to TEMS as **officer**, create the group, and assign the group to a manager.

1. From the **Encryption Center**, select a switch that needs to have a TEMS Client.
2. Select **Properties**.
3. Select the **Key Vault User Name** button.

The **Key Vault User Information** dialog box displays ([Figure 213](#)).



**FIGURE 213** TEMS Key Vault User Information

4. Copy the user name in the **User Name** field.
5. Log in to the Thales management program as a manager who has been assigned to the **brocade** group.
6. Select the **Clients** tab ([Figure 214](#)).

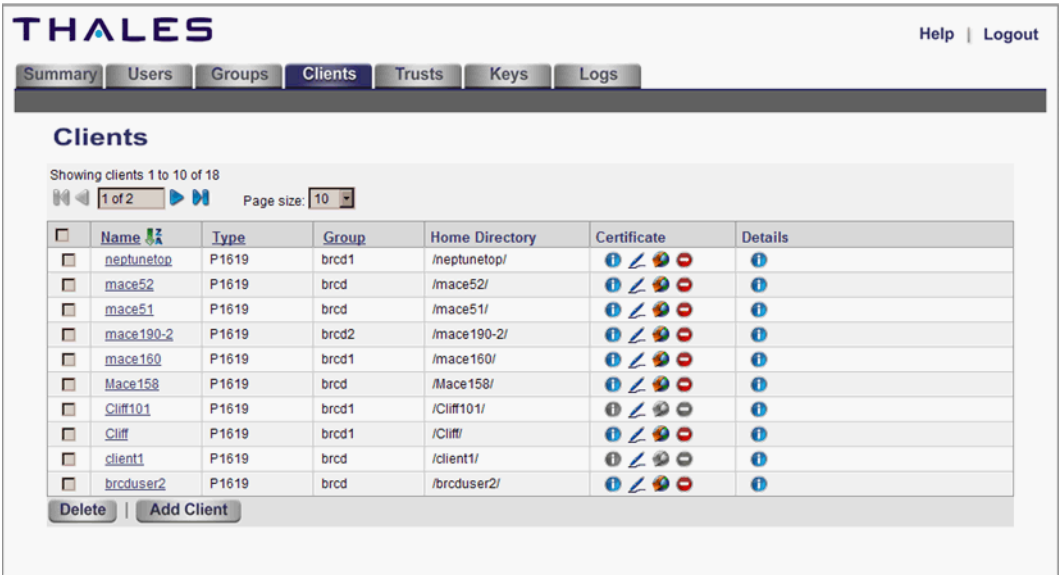


FIGURE 214 TEMS Clients tab

- Click the **Add Client** tab.
- Paste or type in the user name from [step 4](#) in the **Name** field.
- Enter a password in the **Password** and **Verify Password** fields.
- Select the group **brocade** from the group pull down menu.
- Click on **Add Client**.

A TEMS client user is created and is listed in the table.

## Establishing TEMS key vault credentials on the switch

The credentials established for the TEMS client must be presented to TEMS by the switch.

- From the Encryption Center, select **Switch > Key Vault Credentials**.

The Key Vault Credentials dialog box displays ([Figure 215](#)).

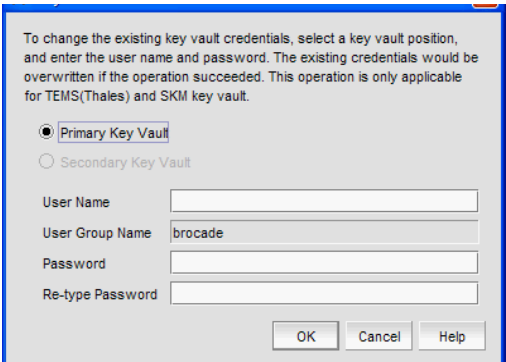


FIGURE 215 Key Vault Credentials

2. Copy exactly the user name and password used when creating the TEMS client.

You may create different credentials, but if you do, you also need to change the TEMS client credentials to match the new credentials.

3. Click **OK**.

## Gathering information

Before you use the encryption setup wizard for the first time, you should also have a detailed configuration plan in place and available for reference. The encryption setup wizard assumes the following:

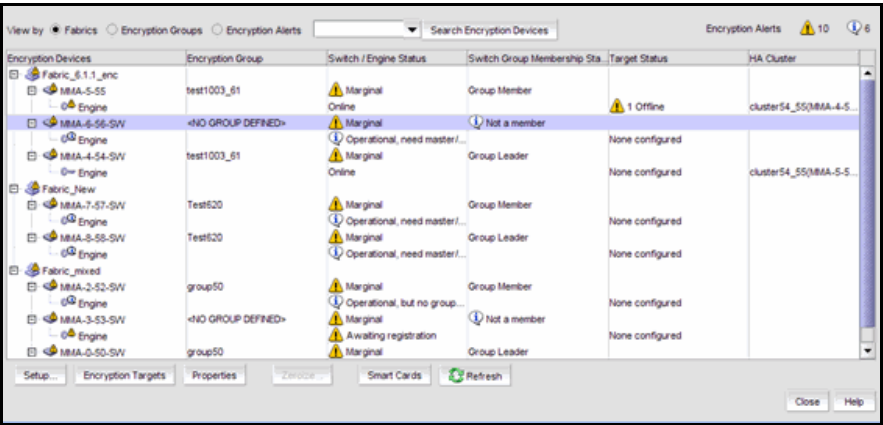
- You have a plan in place to organize encryption devices into encryption groups.
- If you want redundancy and high availability in your implementation you have a plan to create high availability (HA) clusters of two encryption switches or blades to provide failover support.
- All switches in the planned encryption group are interconnected on an I/O synch LAN.
- The management ports on all encryption switches and 384-port Backbone Chassis CPs that have encryption blades installed have a LAN connection to the SAN management program, and are available for discovery.
- A supported key management appliance is connected on the same LAN as the encryption switches, 384-port Backbone Chassis CPs, and the SAN Management program.
- An external host is available on the LAN to facilitate certificate exchange.
- Switch KAC certificates have been signed by a Certificate Authority (CA), and stored in a known location.
- Key management system (key vault) certificates have been obtained and stored in a known location.

# Creating a new encryption group

The following steps describe how to start and run the encryption setup wizard, and then create a new encryption group.

**NOTE**  
When a new encryption group is created, any existing tape pools in the switch are removed.

- 1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.



**FIGURE 216** Encryption Center - No Group Defined dialog box

- 2. Select a switch from the **<NO GROUP DEFINED>** encryption group. The switch must not be in an encryption group already.
- 3. Select a switch and select **Encryption > Create/Add to Group**, from the menu bar, or right-click the switch and select **Create/Add to Group**.

The **Configure Switch Encryption** welcome panel displays.

4. Click **Next**.

**Create a new encryption Group** is pre-selected. This is the correct selection for creating a new group.

**FIGURE 217** Designate Switch Membership dialog box

5. Enter an **Encryption Group Name** for the encryption group (the maximum length of the group name is 15 characters; letters, digits, and underscores are allowed) and select the **Automatic** failback mode.

---

**NOTE**

If the name you enter for the encryption group already exists, a pop-up warning message displays. Although unique group names avoid confusion while managing multiple groups, you are not prevented from using duplicate group names. Click **Yes** to use the same name for the new encryption group, or click **No** to enter a new, unique name.

---

6. Click **Next**.

The **Select Key Vault** dialog box displays ([Figure 218](#)).

## 20 Creating a new encryption group

Steps

Configure Switch Encryption

1. Designate Switch Membership
2. Configure Switch
  - Create a New Encryption Group
  - **Select Key Vault**
  - Select Security Settings
  - Specify Certificate File Name
3. Confirm Configuration

Select Key Vault

Select a key vault type for the encryption group test that will contain switch MMA-4-54-SW.

Key Vault Type

Enter an IP address (IPv4 or hostname) for the primary key vault.

Primary Key Vault

Enter the name of the file holding the primary key vault's public key certificate (Except for Demo Internal key vault).

Primary Certificate File

Optionally, enter a backup key vault address (IPv4 or hostname) and backup certificate file.

Backup Key Vault

Backup Certificate File

**FIGURE 218** Select Key Vault dialog box

7. Select the **Key Vault Type**. The choices are the following:

- RSA Key Manager (RKM)
- NetApp Link Key Manager (LKM)
- HP Secure Key Manager (SKM)
- Thales Encryption Manager for Storage (TEMS)
- Tivoli Key Lifetime Manager (TKLM)

Different options are available depending on which key vault type you choose.

When you select RKM, the options are shown in [Figure 219](#).

- a. Enter the IP address or host name for the primary key vault. If you are clustering RKM appliances for high availability, IP load balancers are used to direct traffic to the appliances. Use the IP address of the load balancer.
- b. Enter the name of the file that holds the primary key vault's public key certificate or browse to the location by clicking the **Browse** button.
- c. If you are implementing encryption on data replication LUNs used by the EMC Symmetrix Remote Data Facility (SRDF), you must select **Enabled** for **REPL Support**.

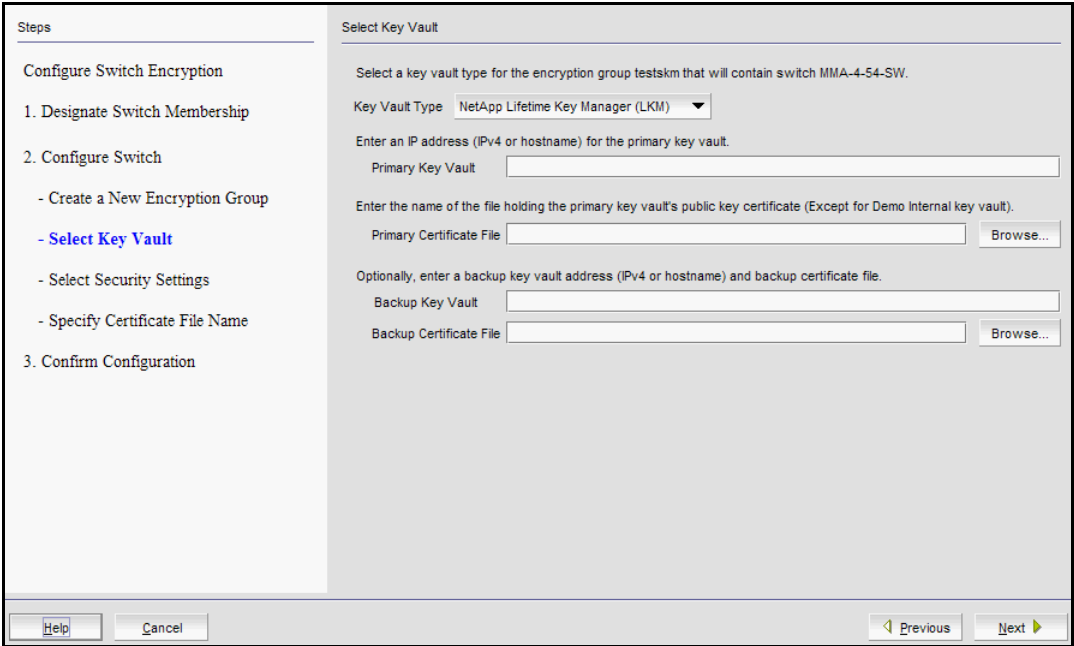
**FIGURE 219** RKM Key Vault Options

- d. Click **Next**.

The **Specify Public Key Certificate File Name** dialog box displays ([Figure 224](#)).

When you select LKM, the options are as shown in [Figure 220](#).

- a. Enter the IP address or host name for the primary key vault.
- b. Enter the name of the file that holds the primary key vault’s public key certificate or browse to the location by clicking the **Browse** button.
- c. If you are using a backup key vault, also enter the IP address or host name, and the name of the file holding the backup key vault’s public key certificate in the fields provided.



**FIGURE 220** LKM Key Vault Options

- d. Click **Next**.

The **Specify Public Key Certificate File Name** dialog box displays ([Figure 224](#)).

When you select SKM, the options are as shown in [Figure 221](#).

- a. Enter the IP address or host name for the primary key vault.
- b. Enter the name of the file that holds the primary key vault's public key certificate or browse to the location by clicking the **Browse** button.
- c. Enter the user name and password you established for the Brocade user group.
- d. If you are using a backup key vault, also enter the IP address or host name, and the name of the file holding the backup key vault's public key certificate in the fields provided. The same user name and password used for the primary key vault are automatically applied to the backup key vault.

The screenshot shows a 'Select Key Vault' dialog box. On the left, a 'Steps' pane lists the configuration process: 'Configure Switch Encryption', '1. Designate Switch Membership', '2. Configure Switch' (with sub-steps '- Create a New Encryption Group', '- Select Key Vault' (highlighted), '- Select Security Settings', and '- Specify Certificate File Name'), and '3. Confirm Configuration'. The main area is titled 'Select Key Vault' and contains the following fields and instructions:

- Instruction: 'Select a key vault type for the encryption group testskm that will contain switch MMA-4-54-SW.'
- Field: 'Key Vault Type' with a dropdown menu showing 'HP Secure Key Manager (SKM)'.
- Instruction: 'Enter an IP address (IPv4 or hostname) for the primary key vault.'
- Field: 'Primary Key Vault'.
- Instruction: 'Enter the name of the file holding the primary key vault's public key certificate and the key vault credentials.'
- Field: 'Primary Certificate File' with a 'Browse...' button.
- Field: 'User Name'.
- Field: 'Password'.
- Field: 'Re-type Password'.
- Instruction: 'Optionally, enter a backup key vault address (IPv4 or hostname), backup certificate file and the key vault credentials.'
- Field: 'Backup Key Vault'.
- Field: 'Backup Certificate File' with a 'Browse...' button.
- Field: 'User Name'.
- Field: 'Password'.
- Field: 'Re-type Password'.

At the bottom, there are 'Help', 'Cancel', 'Previous', and 'Next' buttons.

**FIGURE 221** SKM Key Vault Options

- e. Click **Next**.

The **Specify Public Key Certificate File Name** dialog box displays ([Figure 224](#)).

When you select TEMS, the options are as shown in [Figure 222](#).

- a. Enter the IP address or host name for the primary key vault.
- b. Enter the name of the file that holds the primary key vault’s public key certificate or browse to the location by clicking the **Browse** button.
- c. Enter the user name and password you created for the Brocade group TEMS client.
- d. If you are using a backup key vault, also enter the IP address or host name, the name of the file holding the backup key vault’s public key certificate in the fields provided, and the user name and password for the backup key vault.

**FIGURE 222** TEMS Key Vault Options

- e. Click **Next**.

The **Specify Public Key Certificate File Name** dialog box displays ([Figure 224](#)).

When you select TKLM, the options are as shown in [Figure 223](#).

- a. Enter the IP address or host name for the primary key vault.
- b. Enter the name of the file that holds the primary key vault's public key certificate or browse to the location by clicking the **Browse** button.
- c. If you are using a backup key vault, also enter the IP address or host name and the name of the file holding the backup key vault's public key certificate in the fields provided.

ps

onfigure Switch Encryption

Designate Switch Membership

Configure Switch

- Create a New Encryption Group

- **Select Key Vault**

- Select Security Settings

- Specify Certificate File Name

Confirm Configuration

Select Key Vault

Select a key vault type for the encryption group test that will contain switch switch55.

Key Vault Type IBM Tivoli Key Lifetime Manager (TKLM) ▼

Enter an IP address (IPv4 or hostname) for the primary key vault.

Primary Key Vault

Enter the name of the file holding the primary key vault's public key certificate (Except for Demo Internal key vault).

Primary Certificate File  Browse...

Optionally, enter a backup key vault address (IPv4 or hostname) and backup certificate file.

Backup Key Vault

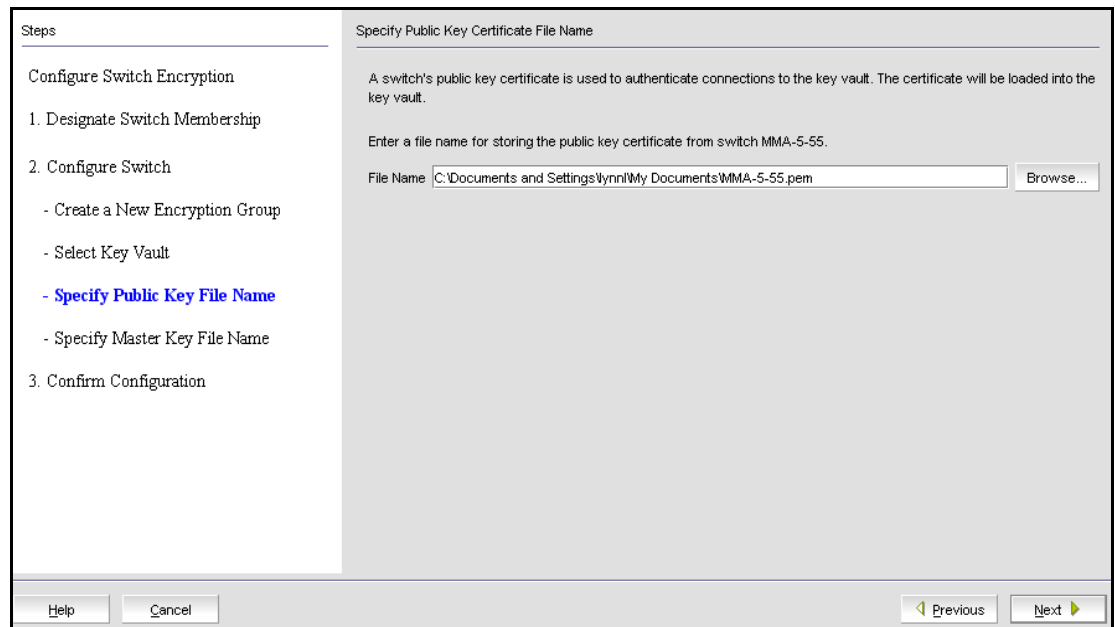
Backup Certificate File  Browse...

Help Cancel Previous Next

**FIGURE 223** TKLM Key Vault Options

- d. Click **Next**.

The **Specify Public Key Certificate File Name** dialog box displays ([Figure 224](#)).



**FIGURE 224** Specify Public Key Certificate filename dialog box

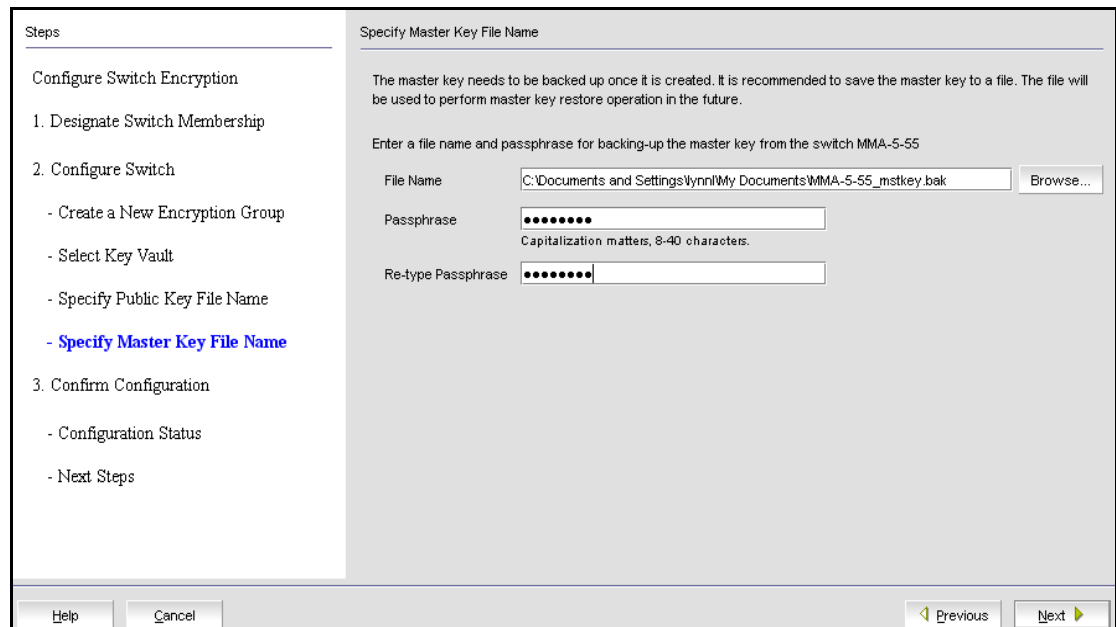
8. Specify the name of the file where you want to store the public key certificate that is used to authenticate connections to the key vault, and click **Next**.

The certificate stored in this file is the switch's public key certificate. You will need to know this path and file name to install the switch's public key certificate on the key management appliance.

9. Click **Next**.

If you chose LKM as the **Key Vault Type**, the **Confirm Configuration** panel displays (skip to [step 14](#)).

For all other supported key vault types, the **Specify Master Key File Name** panel displays ([Figure 225](#)).



The dialog box is titled "Specify Master Key File Name". It features a "Steps" pane on the left and a main configuration area on the right. The "Steps" pane lists the following steps:

- Configure Switch Encryption
  - 1. Designate Switch Membership
  - 2. Configure Switch
    - Create a New Encryption Group
    - Select Key Vault
    - Specify Public Key File Name
    - **Specify Master Key File Name**
  - 3. Confirm Configuration
    - Configuration Status
    - Next Steps

The main configuration area contains the following text and fields:

The master key needs to be backed up once it is created. It is recommended to save the master key to a file. The file will be used to perform master key restore operation in the future.

Enter a file name and passphrase for backing-up the master key from the switch MMA-5-55

File Name:

Passphrase:   
Capitalization matters, 8-40 characters.

Re-type Passphrase:

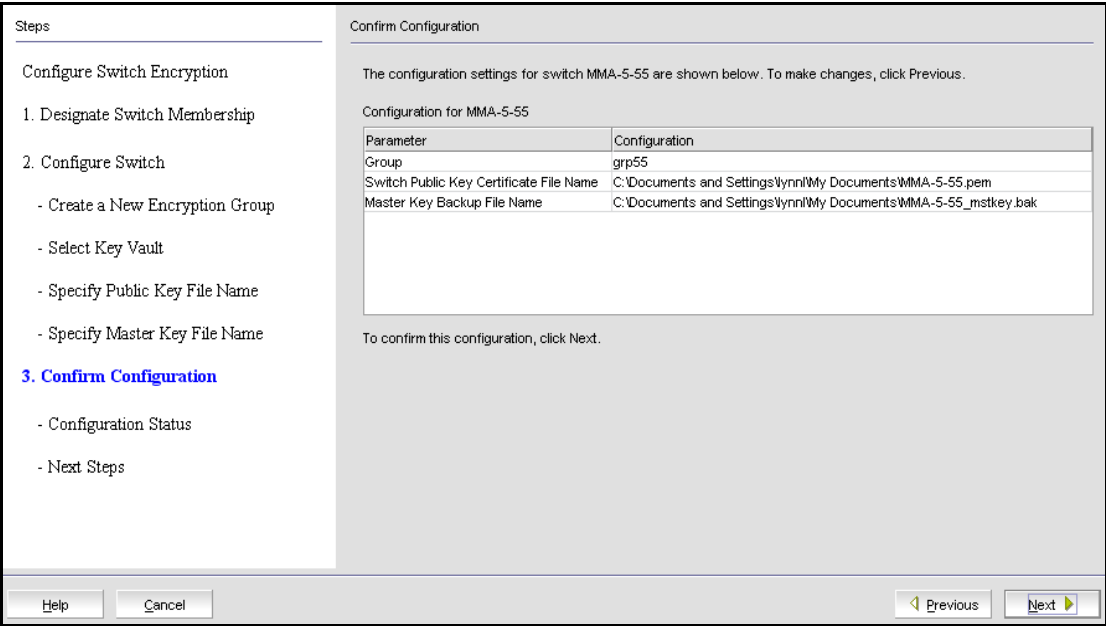
At the bottom, there are buttons for "Help", "Cancel", "Previous", and "Next".

**FIGURE 225** Specify Master Key File Name dialog box

10. Enter a file name, or browse to the desired location.
11. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
12. Re-type the passphrase for verification.

13. Click **Next**.

The **Confirm Configuration** panel displays the encryption group name and switch public key certificate file name you specified, shown in [Figure 226](#).

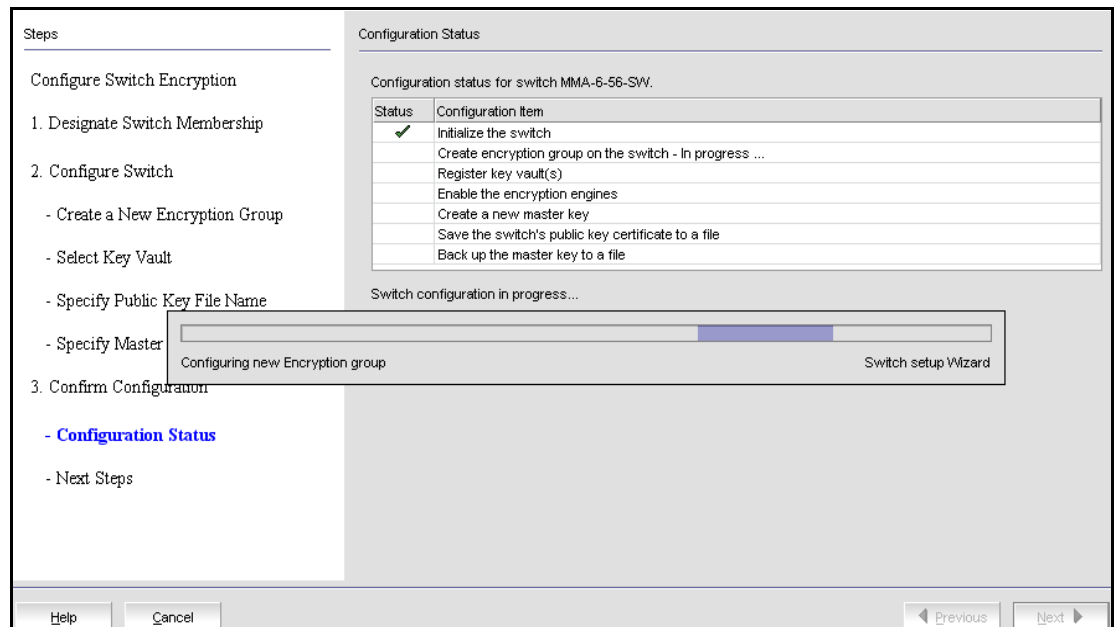


**FIGURE 226** Confirm Configuration dialog box

14. Click **Next** to confirm the displayed information.

The **Configuration Status** displays, as shown in [Figure 227](#). The configuration status steps vary slightly depending on the key vault type.

- A progress indicator shows that a configuration step is in progress. A green check mark indicates successful completion of all steps for that **Configuration Item**. A red stop sign indicates a failed step.
- All **Configuration Items** have green check marks if the configuration is successful. A message displays below the table, indicating that the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.



**FIGURE 227** Configuration Status dialog box

The Management application sends API commands to verify the switch configuration. The CLI commands are detailed in the *Fabric OS Encryption Administrator's Guide*, “Key vault configuration.”

- Initialize the switch**  
 If the switch is not already in the initiated state, the Management application performs the `cryptocfg --initnode` command.
- Create encryption group on the switch**  
 The Management application creates a new group using the `cryptocfg --create -encgroup` command, and sets the key vault type using the `cryptocfg --set -keyvault` command.
- Register key vault(s)**  
 The Management application registers the key vault using the `cryptocfg --reg keyvault` command.
- Enable the encryption engines**  
 The Management application initializes an encryption switch using the `cryptocfg --initEE [<slotnumber>]` and `cryptocfg --regEE [<slotnumber>]` commands.
- Create a new master key**  
 The Management application checks for a new master key. New master keys are generated from the Encryption Group Properties dialog box, Security tab. See “Creating a new master key” on page 568 for more information.

- **Save the switch's public key certificate to a file**

The Management application saves the KAC certificate into the specified file.

- **Back up the master key to a file**

The Management application saves the master key into the specified file. Note that a master key is not generated if the key vault type is LKM. LKM manages DEK exchanges through a trusted link, and the LKM appliance uses its own master key to encrypt DEKs.

15. Click **Next**.

The **Read Instructions** dialog box displays instructions for installing public key certificates for the encryption switch. These instructions are specific to the key vault type. Copy or print these instructions.

16. Click **Finish** to exit the **Configure Switch Encryption** wizard.

At this point, a **Next Steps** dialog box is displayed, with brief instructions that are specific to certificate exchanges between the switch and key manager you are using.

## Adding a switch to an encryption group

The setup wizard allows you to either create a new encryption group, or add an encryption switch to an existing encryption group. Use the following procedure to add a switch to an encryption group.

1. Select **Configure > Encryption** from the menu bar.

The **Encryption Center** dialog box displays.

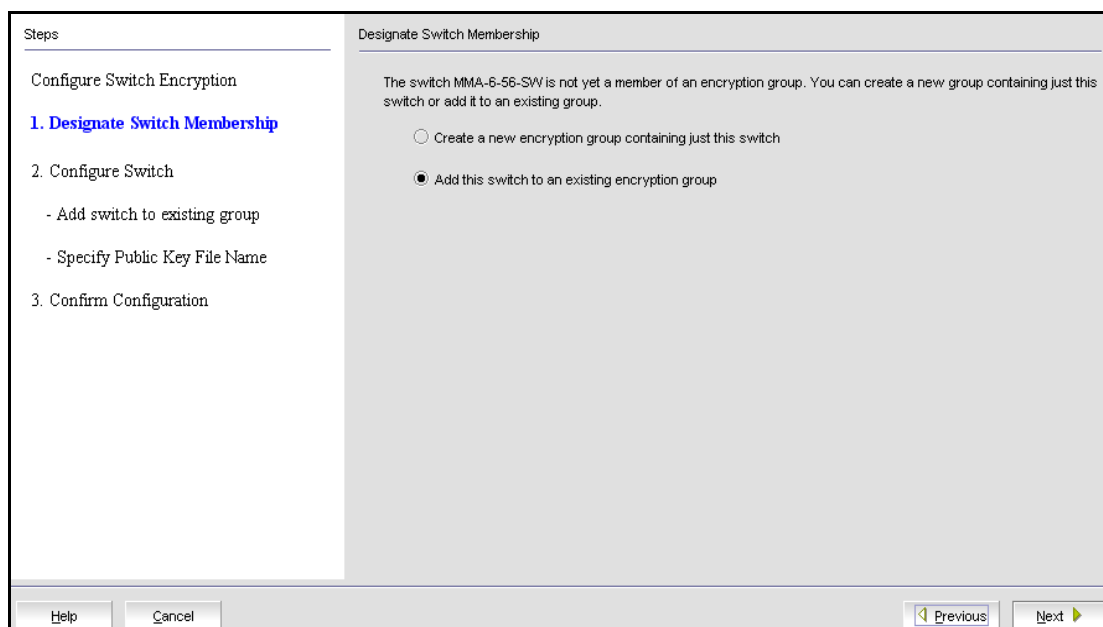
2. Select the switch to be added to the group. The switch must not already be in an encryption group.

3. Select **Switch > Create/Add to Group**, or right-click the switch and select **Create/Add to Group**.

The **Configure Switch Encryption** welcome panel displays.

4. Click **Next**.

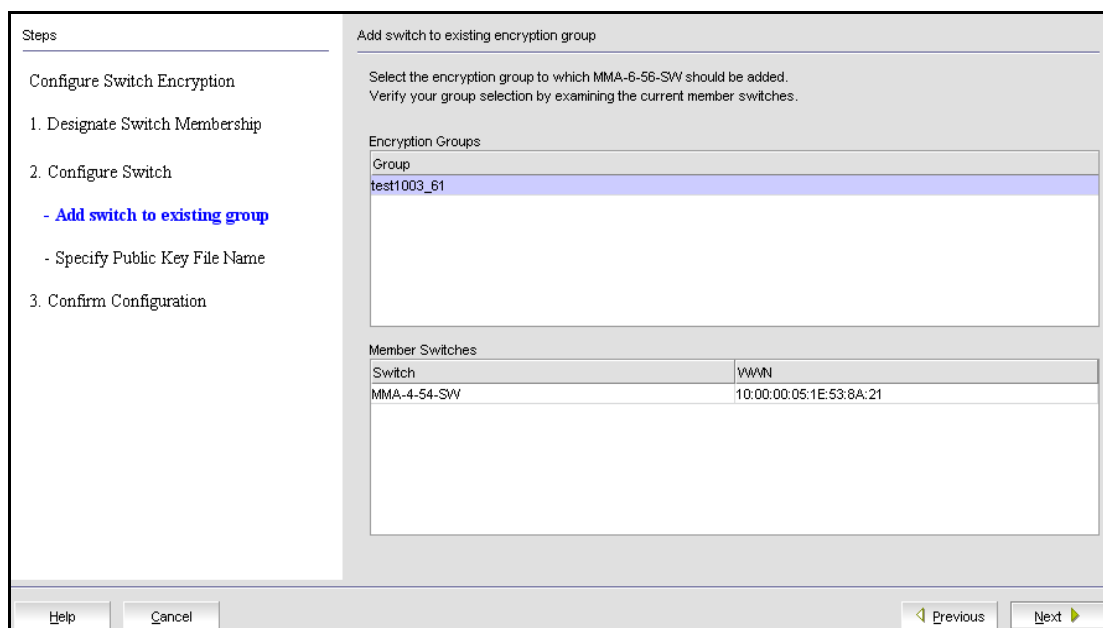
The **Designate Switch Membership** panel displays.



**FIGURE 228** Add switch to an encryption group - Designate Switch Membership dialog box

- a. Select **Add this switch to an existing encryption group**.
- b. Click **Next**.

The **Add Switch to Existing Encryption Group** dialog box displays.

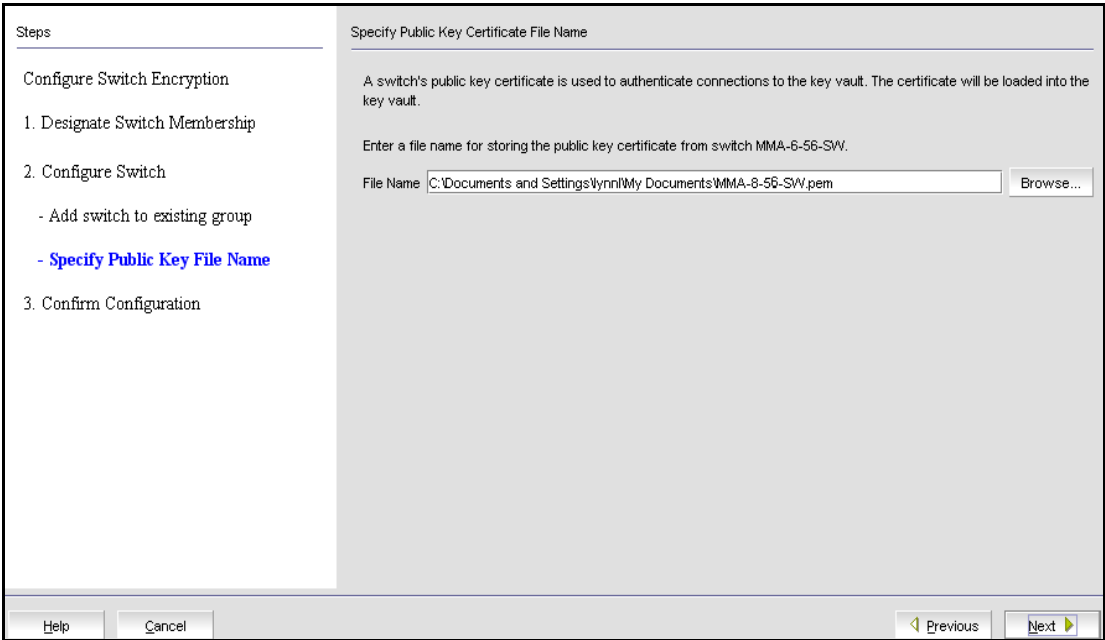


**FIGURE 229** Add Switch to Existing Encryption Group dialog box

5. Select the group to which you want to add the switch, and click **Next**.

The **Specify Public Key Certificate Filename** panel displays.

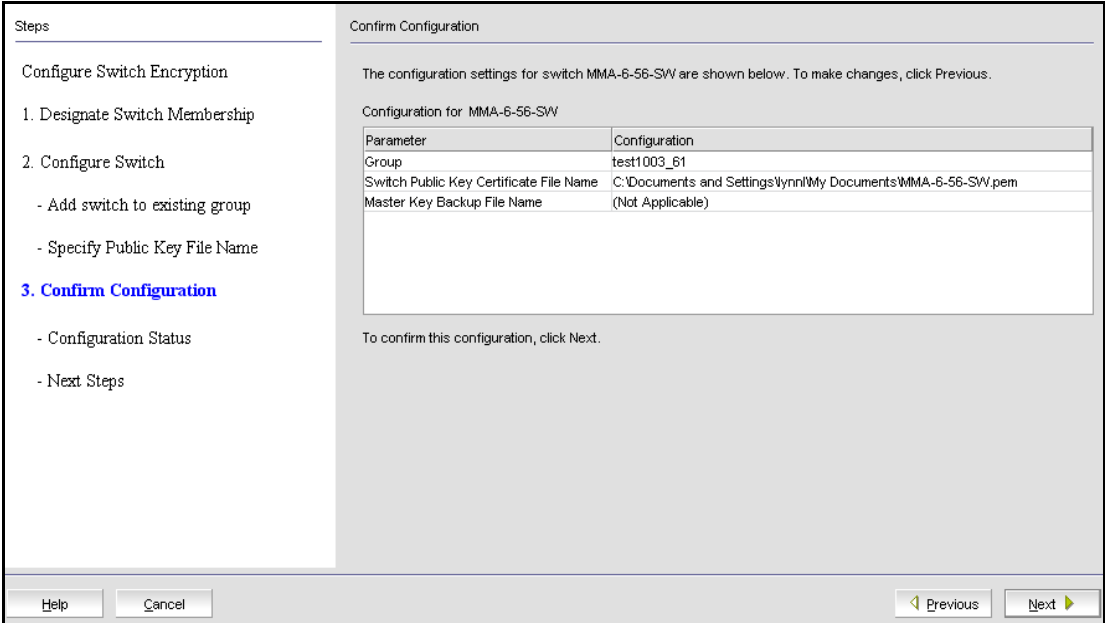
20 Adding a switch to an encryption group



The dialog box is titled "Specify Public Key Certificate File Name". On the left, a "Steps" pane shows the progress: "Configure Switch Encryption" (1. Designate Switch Membership, 2. Configure Switch, 3. Confirm Configuration). Under "2. Configure Switch", the option "- Specify Public Key File Name" is selected. The main area contains instructions: "A switch's public key certificate is used to authenticate connections to the key vault. The certificate will be loaded into the key vault." and "Enter a file name for storing the public key certificate from switch MMA-6-56-SW." Below this is a "File Name" text box containing "C:\Documents and Settings\lynn\My Documents\MMA-6-56-SW.pem" and a "Browse..." button. At the bottom are "Help", "Cancel", "Previous", and "Next" buttons.

FIGURE 230 Add switch to an encryption group - Specify Public Key Certificate filename dialog box

- 6. Specify the name of the file where you want to store the public key certificate that is used to authenticate connections to the key vault, and click **Next**.
- The **Confirm Configuration** panel displays the encryption group name and switch public key certificate file name you specified.



The dialog box is titled "Confirm Configuration". The "Steps" pane on the left shows "3. Confirm Configuration" selected. The main area states: "The configuration settings for switch MMA-6-56-SW are shown below. To make changes, click Previous." Below this is a table showing the configuration for MMA-6-56-SW.

| Parameter                               | Configuration                                               |
|-----------------------------------------|-------------------------------------------------------------|
| Group                                   | test1003_61                                                 |
| Switch Public Key Certificate File Name | C:\Documents and Settings\lynn\My Documents\MMA-6-56-SW.pem |
| Master Key Backup File Name             | (Not Applicable)                                            |

Below the table, it says "To confirm this configuration, click Next." At the bottom are "Help", "Cancel", "Previous", and "Next" buttons.

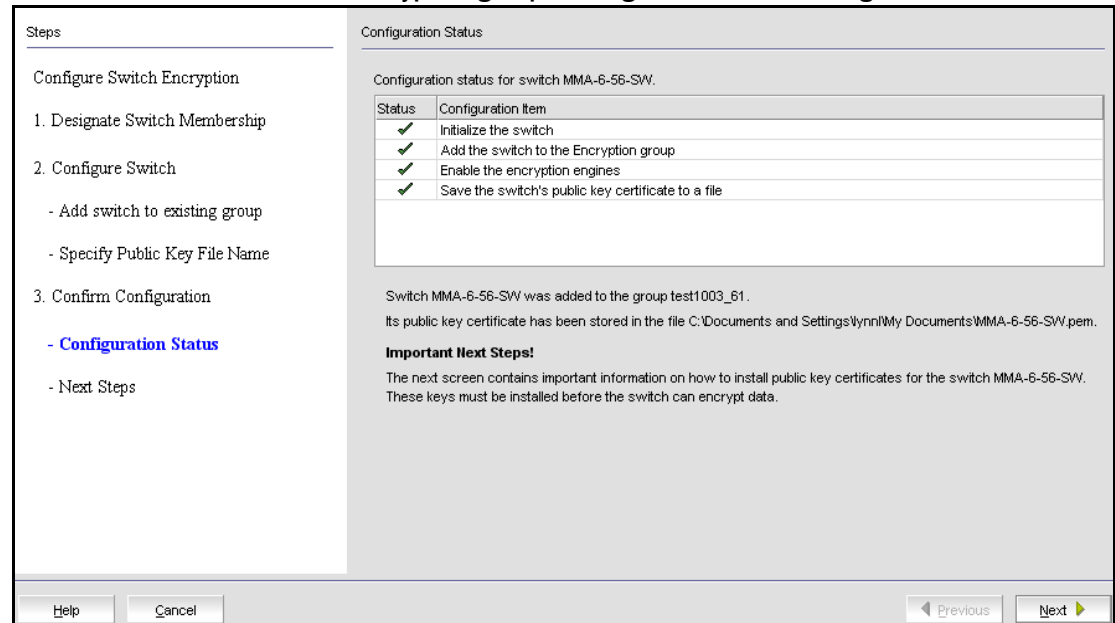
FIGURE 231 Add switch to an encryption group - Confirm Configuration dialog box

7. Click **Next** to confirm the displayed information.

The **Configuration Status** displays.

- A progress indicator shows that a configuration step is in progress. A green check mark indicates successful completion of all steps for that **Configuration Item**. A red stop sign indicates a failed step.
- All **Configuration Items** have green check marks if the configuration is successful. A message displays below the table, indicating that the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.

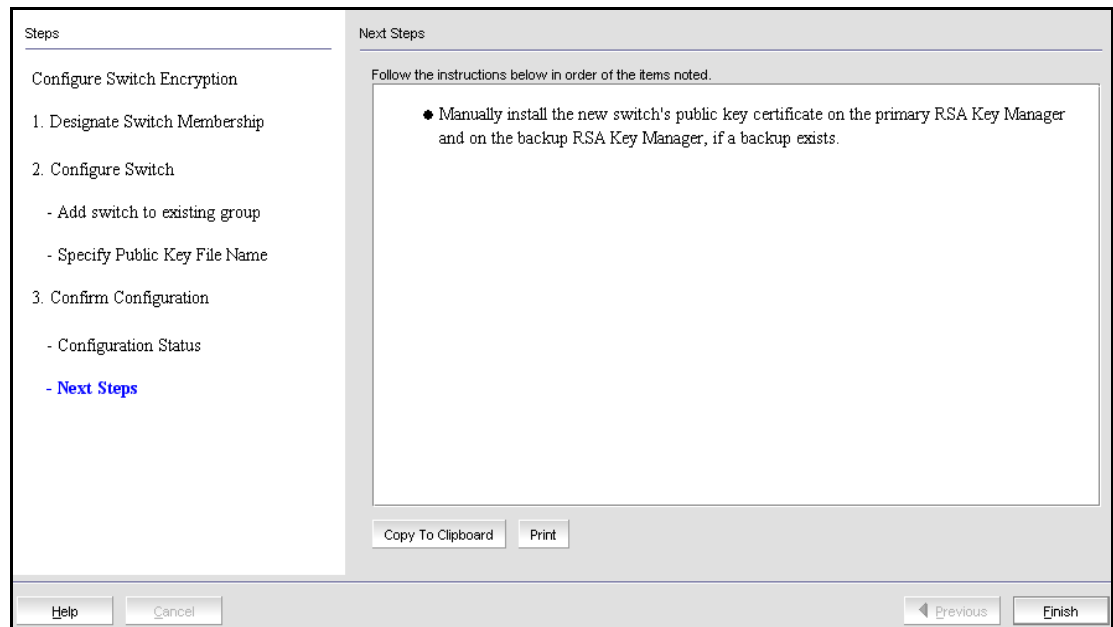
**FIGURE 232** Add switch to an encryption group - Configuration Status dialog box



8. Note **Important Next Steps!** below this message, and click **Next**.

Instructions for installing public key certificates for the encryption switch are displayed. These instructions are specific to the key vault type. Copy or print these instructions.

## 20 Replacing an encryption engine in an encryption group



**FIGURE 233** Add switch to an encryption group - Next Steps dialog box

9. Click **Finish** to exit the **Configure Switch Encryption** wizard.

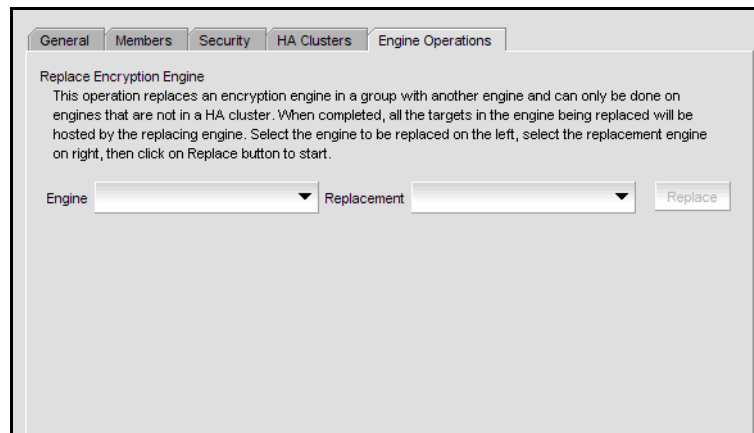
## Replacing an encryption engine in an encryption group

To replace an encryption engine in an encryption group with another encryption engine within the same DEK Cluster, complete the following steps.

1. From the Encryption Center, select the encryption engine, and select **Engine > Replace**, or right click on the encryption engine and select **Replace**.

The **Engine Operations** tab of the **Encryption Group Properties** dialog box displays (Figure 234).

You can also display the **Engine Operations** tab by selecting an encryption group from the tree, and selecting **Group > Properties** from the menu bar and selecting the **Engine Operations** tab, or you can right-click the encryption group, select **Properties** and select the **Engine Operations** tab.



**FIGURE 234** Engine Operations tab

2. Select the engine you want to replace in the **Engine** list.
3. Select the engine you want to use as the replacement in the **Replacement** list.
4. Click **Replace**.

All containers hosted by the current engine (**Engine** list) are replaced by the new engine (**Replacement** list).

## Creating high availability (HA) clusters

A high availability (HA) cluster is a group of exactly two encryption engines. One encryption engine can take over encryption and decryption tasks for the other encryption engine, if that member fails or becomes unreachable.

When creating a new HA Cluster, add one engine to create the cluster and then add the second engine. You can make multiple changes to the HA Clusters list; the changes are not applied to the switch until you click **OK**.

Both engines in an HA cluster must be in the same fabric as well as the same encryption group.

### NOTE

An IP address is required for the management port for any cluster-related operations.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. If groups are not visible in the **Encryption Devices** table, select **View > Groups** from the menu bar.  
The encryption groups display in the **Encryption Devices** table.
3. Select an encryption group from the tree, and select **Group > HA Cluster** from the menu bar, or right-click the encryption group and select **HA Cluster**.

**Encryption Group Properties** are displayed, with the **HA Clusters** tab selected (Figure 235). Available encryption engines are listed under **Non-HA Encryption Engines**.

- 4. Select an available encryption engine, and a destination HA cluster under **High-Availability Clusters**. Select **New HA Cluster** if you are creating a new cluster.
- 5. Click the right arrow to add the encryption engine to the selected HA cluster.

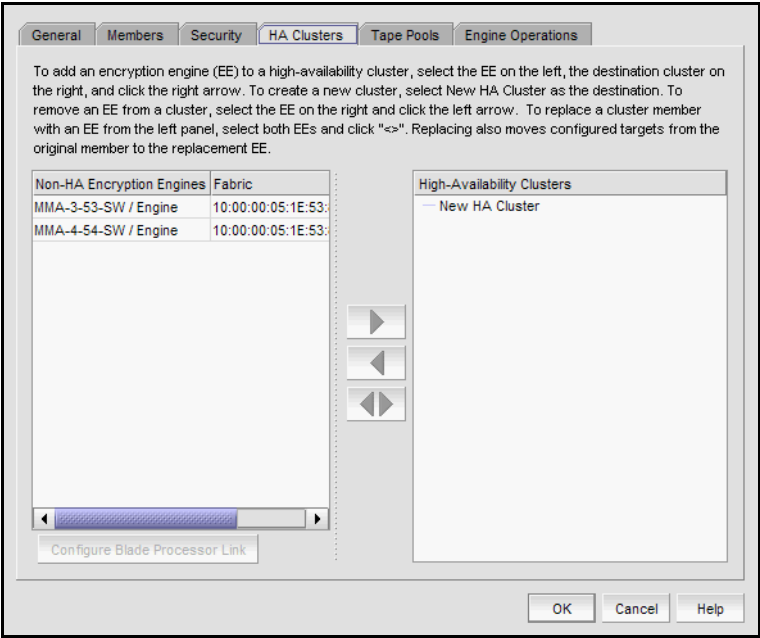


FIGURE 235 HA Clusters tab

**NOTE**  
If you are creating a new HA cluster, a dialog box displays requesting a name for the new HA cluster. HA Cluster names can have up to 31 characters. Letters, digits, and underscores are allowed.

## Removing engines from an HA cluster

- Removing the last engine from an HA cluster also removes the HA cluster.
- If only one engine is removed from a two-engine cluster, you must either add another engine to the cluster or the other engine must be removed too.
- 1. Select an encryption engine from the right tree (see [Figure 235](#)) and click the left arrow button.
  - 2. Either remove the second engine or add a replacement second engine, making sure all HA clusters have exactly two engines.
  - 3. Click **OK**.

## Swapping engines in an HA cluster

Swapping engines is useful when replacing hardware. Swapping engines is different from removing an engine and adding another because when you swap engines, the configured targets on the former HA cluster member are moved to the new HA cluster member.

To swap engines, select one engine from the right tree (see [Figure 235](#)) and one unclustered engine from the list on the left, and click the double-arrow button.

---

**NOTE**

The two engines being swapped must be in the same fabric.

---

## Failback option

The **Failback** option determines the behavior when a failed encryption engine is restarted. When the first encryption engine comes back online, the encryption group's failback setting (auto or manual) determines how the encryption engine resumes encrypting and decrypting traffic to its encryption targets.

- In auto mode, when the first encryption engine restarts, it automatically resumes encrypting and decrypting traffic to its encryption targets.
- In manual mode, the second encryption engine continues handling the traffic until you manually invoke failback using the CLI or Management application, or until the second encryption engine fails.

## Invoking failback

To invoke failback to the restarted encryption engine from the Management application, complete the following steps.

1. Select **Configure > Encryption**.

The **Encryption Center** dialog box displays.

2. Select the group to which the encryption engine belongs from the **Encryption Devices** table, and click **Properties**.

The **Encryption Group Properties** dialog box displays.

3. Click the **HA Clusters** tab.
4. Select the online encryption engine and click **Failback**.
5. Click **OK** on the **Encryption Group Properties** dialog box.
6. Click **Close** on the **Encryption Center** dialog box.

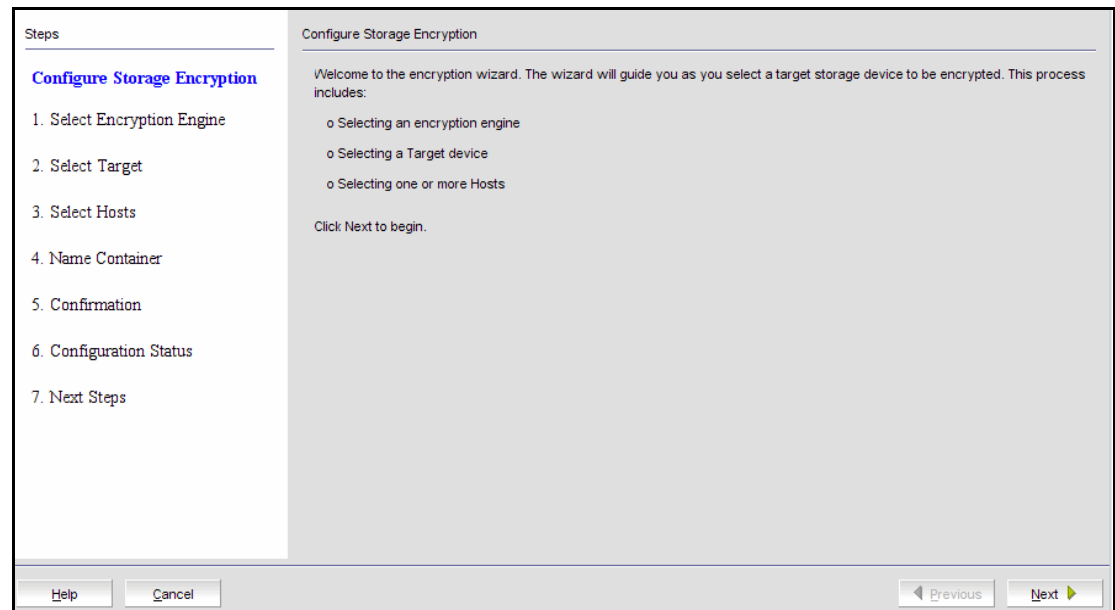
## Adding encryption targets

Adding an encryption target maps storage devices and hosts to virtual targets and virtual initiators within the encryption switch.

### NOTE

It is recommended that you zone the host and target together before configuring them for encryption. If the host and target are not already zoned, you can still configure them for encryption, but afterward you will need to zone the host and target together, and then click the **Commit** button to commit the changes. If you attempt to close the Encryption Targets dialog box without committing the changes, you are reminded of uncommitted changes in the Management application.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Select the encryption group, switch, or encryption engine to which you want to add the target. Right-click, or select **Group**, **Switch**, or **Engine** from the menu bar.
3. Select **Targets**.  
The **Encryption Targets** dialog box displays.
4. Click **Add**.  
The **Configure Storage Encryption** welcome panel displays. The welcome panel explains the wizard's purpose, which is to configure encryption for a storage device (target).

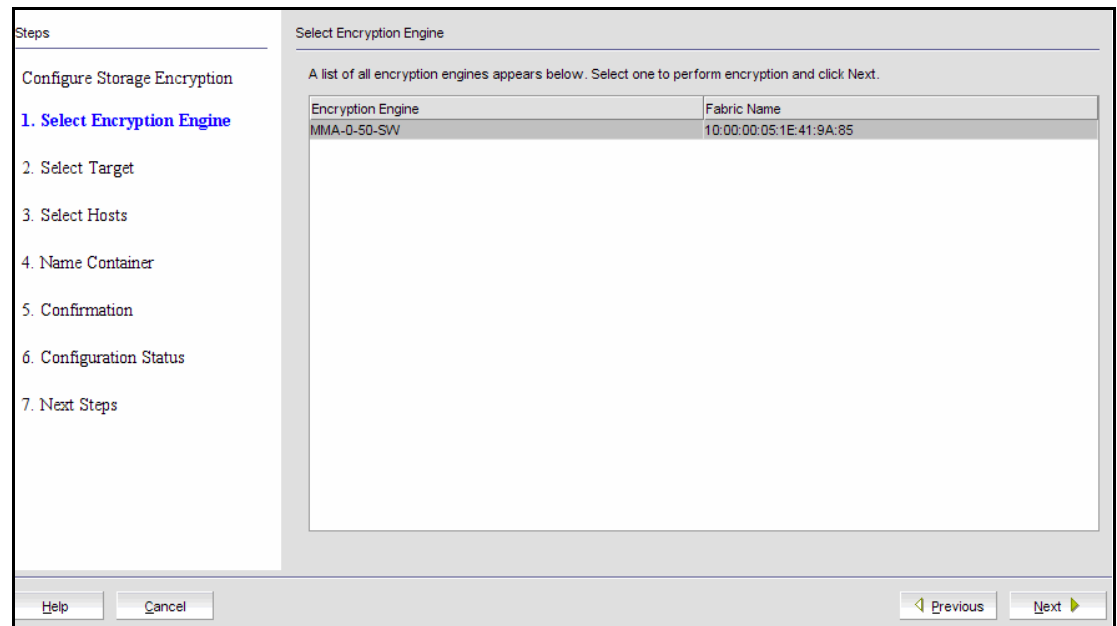


**FIGURE 236** Configure Storage Encryption welcome panel

5. Click **Next** to begin.

The **Select Encryption Engine** dialog box displays. The list of engines depends on the scope being viewed.

- If the Targets dialog box is showing all targets in an encryption group, the list includes all engines in the group.
- If the Targets dialog box is showing all targets for a switch, the list includes all encryption engines for the switch.
- If the Targets dialog box is showing targets for a single encryption engine, the list contains only that engine.



**FIGURE 237** Select Encryption Engine dialog box

6. Select the encryption engine (blade or switch) you want to configure, and click **Next**.

The **Select Target** panel displays. This panel lists all target ports and target nodes in the same fabric as the encryption engine. The **Select Target** list does *not* show targets that are already configured in an encryption group.

There are two available methods for selecting targets: select from the list of known targets or manually enter the port and node WWNs.

Steps

Configure Storage Encryption

1. Select Encryption Engine

2. Select Target

3. Select Hosts

4. Name Container

5. Confirmation

6. Configuration Status

7. Next Steps

Select Target

You have chosen to configure a target for encryption engine 10:00:00:05:1E:41:9A:85 in switch MMA-0-50-SW in the 10:00:00:05:1E:41:9A:85 fabric. All target device port WWNs in that fabric appear below. Select a target, or enter a PORT WWN and a Node WWN in the fields below the table. Then select the target type. For information on MPIO-based configurations, click Help. When ready, click Next.

Targets in Fabric

| Port WWN                | Port Name                                 | Node WWN                |
|-------------------------|-------------------------------------------|-------------------------|
| 50:01:10:A0:00:8B:F6:0B | HP Ultrium 3 Fibre Channel S/N-HU10739... | 50:01:10:A0:00:8B:F6:09 |
| 50:01:10:A0:00:8B:F6:0A | HP Ultrium 3 Fibre Channel S/N-HU10739... | 50:01:10:A0:00:8B:F6:09 |
| 21:00:00:20:37:F2:C2:04 | SEAGATE ST318451FC F26D                   | 20:00:00:20:37:F2:C2:04 |
| 21:00:00:20:37:EC:72:0C | SEAGATE ST318451FC F28D                   | 20:00:00:20:37:EC:72:0C |
| 21:00:00:20:37:F2:BE:12 | SEAGATE ST318451FC F26D                   | 20:00:00:20:37:F2:BE:12 |
| 21:00:00:20:37:E8:47:31 | SEAGATE ST318451FC F28D                   | 20:00:00:20:37:E8:47:31 |
| 21:00:00:20:37:F5:B3:9A | SEAGATE ST318451FC F28D                   | 20:00:00:20:37:F5:B3:9A |
| 21:00:00:20:37:F2:BD:F8 | SEAGATE ST318451FC F26D                   | 20:00:00:20:37:F2:BD:F8 |
| 20:04:00:A0:B8:1F:C5:0F | LSI INF-01-00 0612                        | 20:04:00:A0:B8:1F:C5:0D |
| 20:04:00:A0:B8:1F:C5:0E | LSI INF-01-00 0612                        | 20:04:00:A0:B8:1F:C5:0D |
| 50:06:01:62:10:60:06:3A | DGC LUNZ 0219                             | 50:06:01:60:90:60:06:3A |
| 10:00:00:06:2B:0C:C8:54 | LSI7202XP-LC A.1 03-00021-02B FW:01.....  | 20:00:00:06:2B:0C:C8:54 |
| 10:00:00:06:2B:0D:30:50 | LSI7204XP-LC A.1 03-01078-02F FW:01.....  | 20:00:00:06:2B:0D:30:50 |

Port WWN

Node WWN

Type

Select

Help

Cancel

Previous

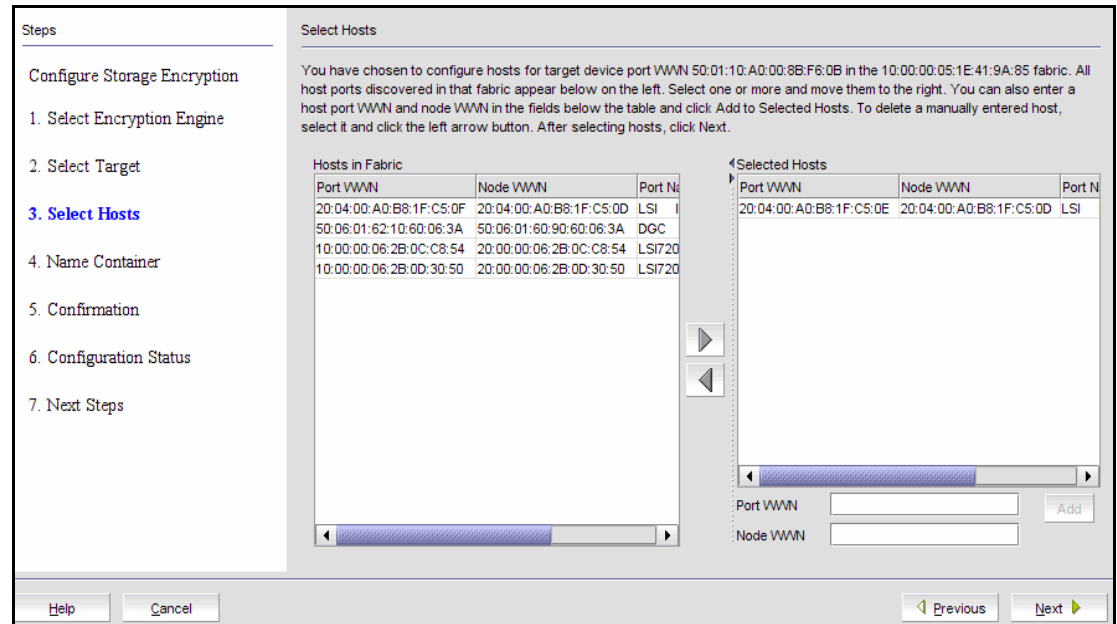
Next

FIGURE 238 Select Target dialog box

- a. Select a target from the list. (The **Target Port WWN** and **Target Node WWN** fields contain all the target information that displays using the `sshshow` command.) You can also enter WWNs manually if you prefer, or if you want to specify a target that is not on the list.
- b. Select a **Target Type**. If the target node is disk storage, choose **Disk**. If the target node is tape storage, choose **Tape**.

7. Click **Next**.

The **Select Hosts** panel displays. This panel lists all hosts in the same fabric as the encryption engine. There are two available methods for selecting hosts: select from a list of known hosts or manually enter the port and node world wide names.



**FIGURE 239** Select Hosts dialog box

- Select a maximum of 1024 hosts from the **Host Ports in Fabric** list, and click the right arrow to move the host to the **Selected Hosts** list. (The **Host Port WWN** column contains all the target information that displays using the `nsshow` command.)
  - Manually enter world wide names in the **Host Port WWN** and **Host Port WWN** text boxes, if the hosts are not included in the list. You must fill in both the Host Port WWN and the Host Node WWN. Click the **Add to Selected Hosts** button to move the host to the **Selected Hosts** list.
8. Click **Next** when you are finished selecting hosts or manually entering the WWNs.

The **Name Container** panel displays.

The name container step in the wizard enables you to specify a name for the target container that is created in the encryption engine to hold the target configuration data.

- The container name defaults to the target WWP. You can, however, rename the container name. If you want to specify a name other than the default, enter a name, using a maximum number of 31 characters. Letters, digits, and underscores are allowed.

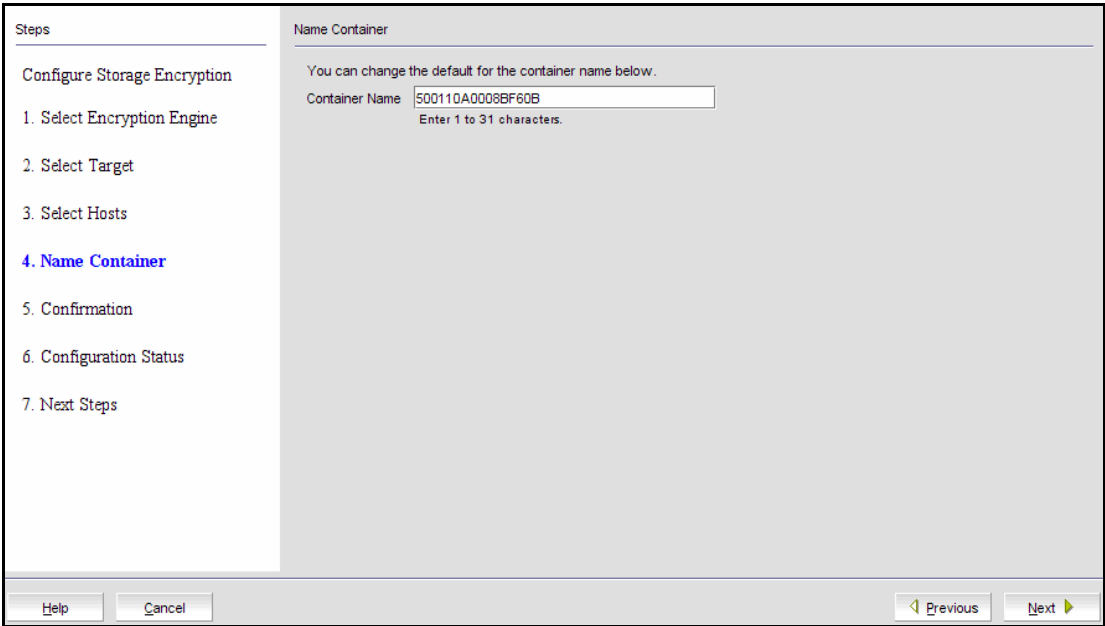


FIGURE 240 Name Container dialog box

10. Click **Next**.
- The **Confirmation** panel displays.

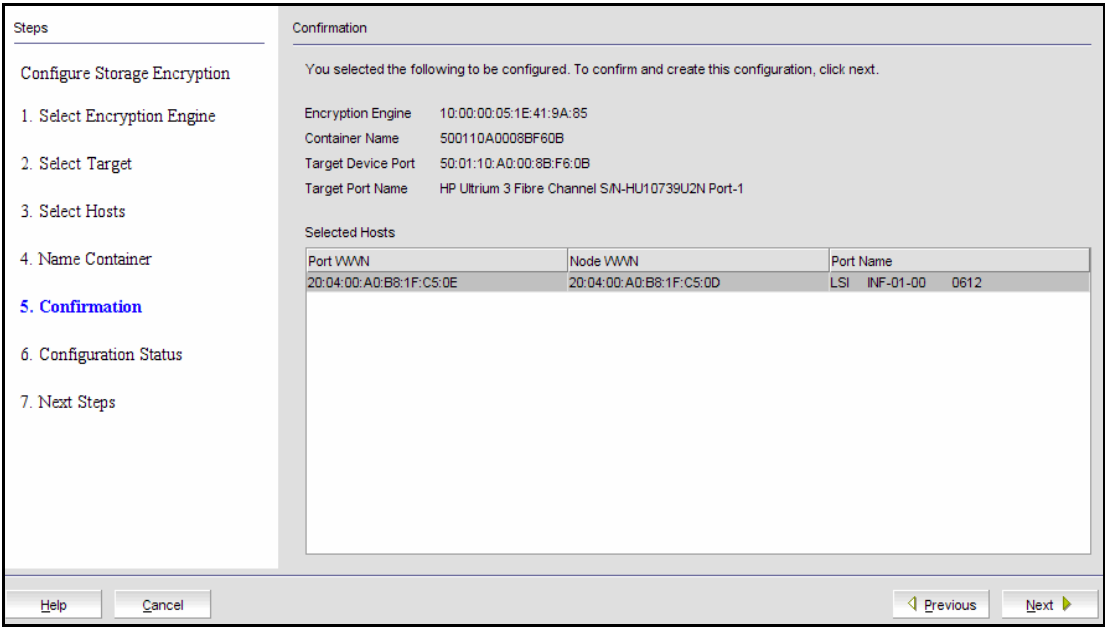
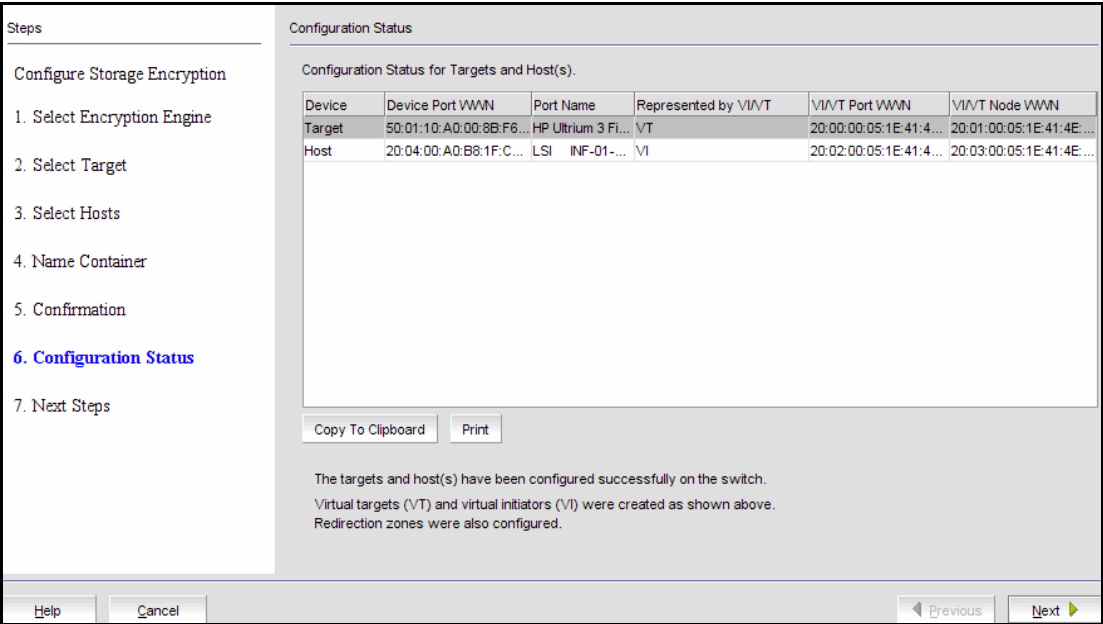


FIGURE 241 Confirmation dialog box

11. Click **Next** to confirm the displayed information.

The **Configuration Status** displays the target and host that are configured in the target container, as well as the virtual targets (VT) and virtual initiators (VI).

**NOTE**  
If you can view the VI/VT Port WWNs and VI/VT Node WWNs, the container has been successfully added to the switch.

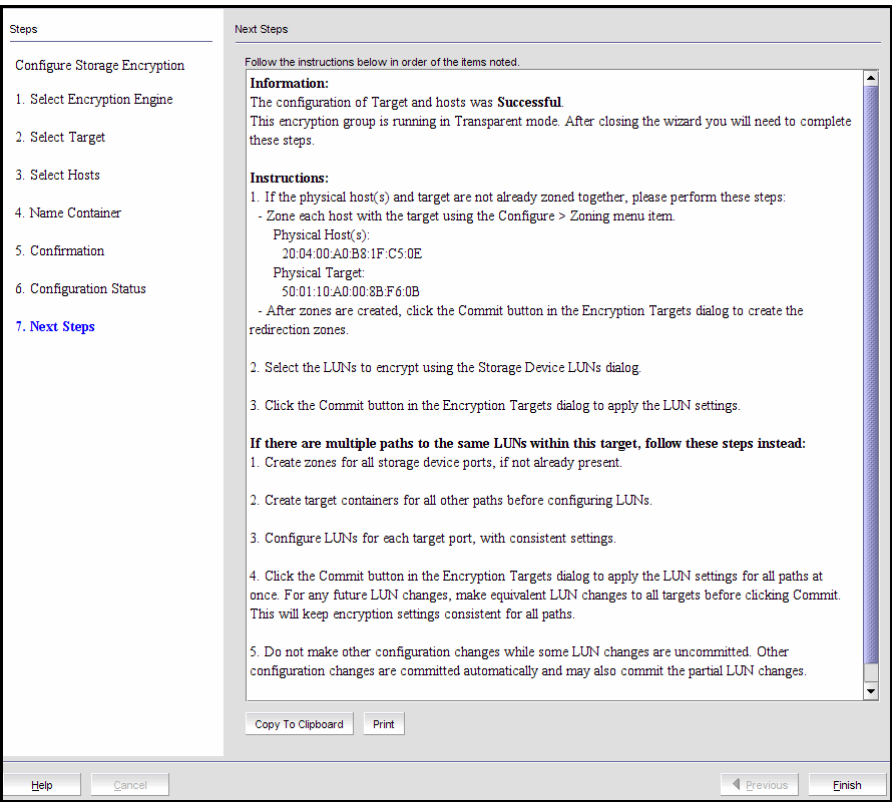


**FIGURE 242** Configuration Status dialog box

12. Review the configuration. If you want to save a copy of the instructions, click the **Copy to Clipboard** button.

13. Click **Next** to confirm the configuration.

The **Important Instructions** dialog box displays.



**FIGURE 243** Important Instructions dialog box

14. Review the instructions about post-configuration tasks you must complete after you close the wizard.

15. Click **Finish** to exit the **Configure Storage Encryption** wizard.

## Configuring hosts for encryption targets

Use the **Encryption Target Hosts** dialog box to edit (add or remove) hosts for an encrypted target.

### NOTE

Hosts are normally selected as part of the **Configure Storage Encryption** wizard but you can also edit hosts later using the **Encryption Target Hosts** dialog box.

1. Select **Configure > Encryption** from the menu bar.

The **Encryption Center** dialog box displays.

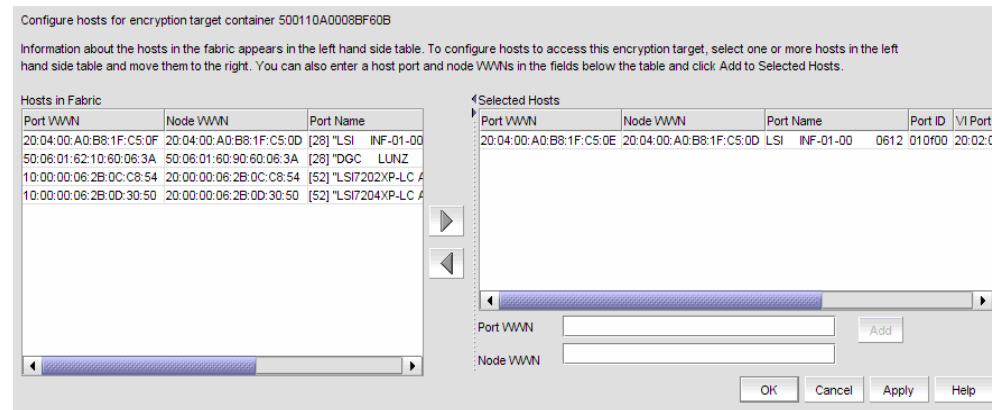
2. Select the encryption group, switch, or encryption engine containing the storage device to be configured. Right-click, or select **Group**, **Switch**, or **Engine** from the menu bar.
3. Select **Targets**.

The **Encryption Targets** dialog box displays.

4. Select a Target storage device from the list, and click **Hosts**.

The **Encryption Target Hosts** dialog box displays. This dialog box lists configured hosts in a fabric.

5. Select one or more hosts in a fabric and move them to the **Selected Hosts** table.



**FIGURE 244** Encryption Target Hosts dialog box

# Adding target disk LUNs for encryption

You can add a new path to an existing disk LUN or add a new LUN and path by launching the **Add New Path** wizard. Take the following steps to launch the **Add New Path** wizard.

- 1. Select **Configure > Encryption**.  
The **Encryption Center** dialog box displays.
- 2. Right-click a group, switch, or encryption engine or select a group, switch, or encryption engine from the **Encryption Devices** table and select **Disk LUNs**.  
The **Encryption Disk LUN** view displays (Figure 245).



FIGURE 245 Encryption Disk LUN view

- 3. Select **Add**.  
The **Add New Path** wizard **Select Target Port** dialog box displays (Figure 246).

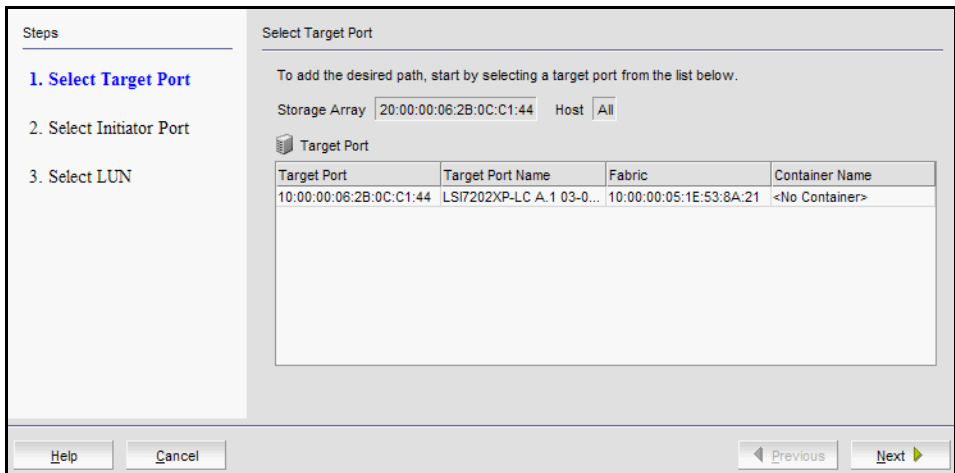


FIGURE 246 Add New Path Wizard

- 4. Select the target port from the **Target Port** list.

5. Click **Next**.

The **Select Initiator Port** dialog box displays.

6. Select the initiator port from the **Initiator Port** list.
7. Click **Next**.

LUN discovery is launched, and a progress bar displays. There are four possible outcomes:

- A message displays indicating No LUNs are discovered. Click **OK** to dismiss the message and exit the wizard.
- A message displays indicating LUNs are discovered, but are already configured. Click **OK** to dismiss the message and exit the wizard.
- A message displays indicating that the target is not in the right state for discovering LUNs. Click **OK** to dismiss the message and exit the wizard.
- The **Select LUN** dialog box displays, showing discovered LUNs that are available.

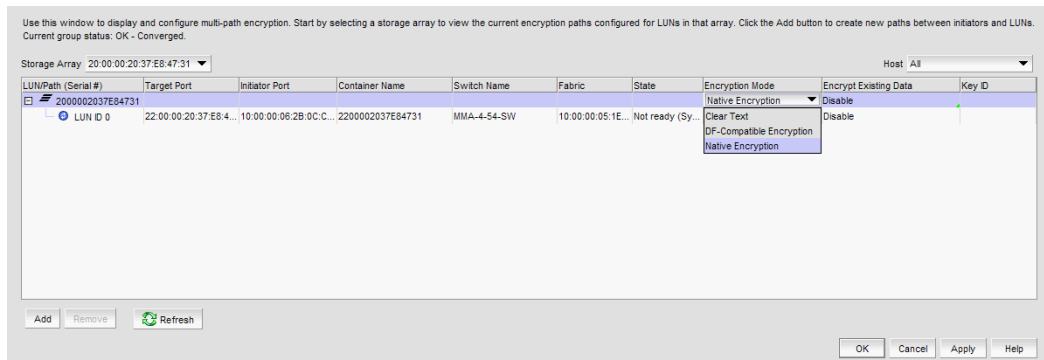
8. Select the LUN from **LUN** list.

9. If **REPL Support** was enabled by the **Configure Switch Encryption** wizard, a **New LUN** checkbox is presented and enabled by default. If this LUN is to be paired with another LUN for SRDF data replication, the **New LUN** option must be enabled by selecting this checkbox. Refer to [“Metadata requirements and remote replication”](#) for information about how this option works. If **REPL support** was not enabled, this checkbox is not displayed.

10. Click **Finish**.

The new LUN path is added to the **Encryption Disk LUN** view.

11. In environments where there are multiple paths to the same LUNs, it is critical that the same LUN policies are configured on all instances of the LUN. Be sure to return to the **Encryption Disk LUN** view to determine if there are configuration mismatches. Check under **Encryption Mode** for any entries showing **Mismatch**. You can correct the mismatch by clicking on the incorrect mode to display the choices, and selecting the correct mode ([Figure 247](#)).



**FIGURE 247** Correcting an Encryption Mode Mismatch

When you correct a policy on a LUN, it is automatically selected for all paths to the selected LUN. When you modify LUN policies, a Modify icon appears to identify the modified LUN entry.

12. Click **Add** or **Apply** to apply the modifications.

## Remote replication LUNs

The Symmetrix Remote Data Facility (SRDF) transmits data that is being written to a local Symmetrix array to a remote symmetrix array. The replicated data facilitates a fast switchover to the remote site for data recovery.

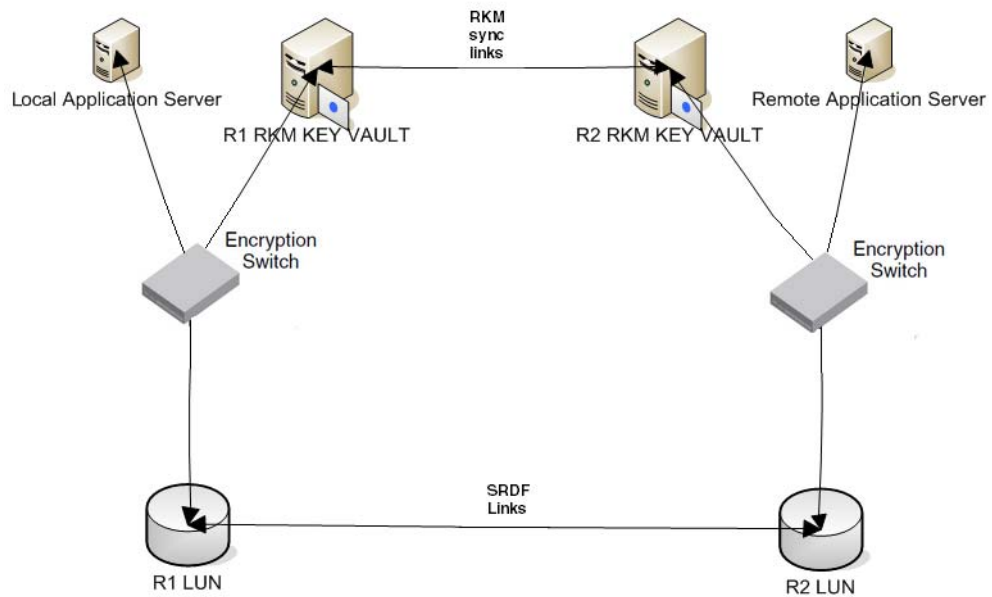
SRDF supports the following methods of data replication:

- Synchronous Replication provides real-time mirroring of data between the source Symmetrix and the target Symmetrix systems. Data is written simultaneously to the cache of both systems in real time before the application I/O is completed, thus ensuring the highest possible data availability.
- Semi-Synchronous Replication writes data to the source system, completes the I/O, and then synchronizes the data with the target system. Since the I/O is completed prior to synchronizing data with the target system, this method provides an added performance advantage. A second write will not be accepted on a Symmetrix source device until its target device has been synchronized.
- Adaptive Copy Replication transfers data from the source devices to the remote devices without waiting for an acknowledgment. This is especially useful when transferring large amounts of data during data center migrations, consolidations, and in data mobility environments.
- Asynchronous Replication places host writes into chunks and then transfers an entire chunk to the target system. When a complete chunk is received on the target system, the copy cycle is committed. If the SRDF links are lost during data transfer, any partial chunk is discarded, preserving consistency on the target system. This method provides a consistent point-in-time remote image that is not far behind the source system and results in minimal data loss if there is a disaster at the source site.

## SRDF pairs

Remote replication is implemented by establishing a synchronized pair of SRDF devices connected by FC or IP links. A local source device is paired with a remote target device while data replication is taking place. While the SRDF devices are paired, the remote target device is not locally accessible for read or write operations. When the data replication operation completes, the pair may be split to enable normal read/write access to both devices. The pair may be restored to restore the data on the local source device.

[Figure 248](#) shows the placement of Brocade encryption switches in an SRDF configuration. When encryption is enabled for the primary LUN, encrypted data written by the local application server to the primary LUN is replicated on the secondary LUN. The data is encrypted using a DEK that was generated on the local encryption switch and stored on the local RKM key vault. When each site has an independent key vault, as shown in [Figure 248](#), the key vaults must be synchronized to ensure the availability of the DEK at the remote site. Refer to RKM user documentation for information about how to synchronize the key vaults. Both sites may share the same key vault, which eliminates the need for synchronization across sites. Depending on distance between sites, sharing a key vault may add some latency when retrieving a key.



**FIGURE 248** Basic SRDF configuration with Brocade encryption switches

## Metadata requirements and remote replication

When the metadata and key ID are written, the primary metadata on blocks 1 to 16 is compressed and encrypted. However, there are scenarios where these blocks are not compressible, and the metadata is not written to the media. If blocks 1 to 16 are not compressible on local source device and metadata is not written, obtaining the correct DEK for the remote target device becomes problematic. This problem is avoided by reserving the last three blocks of the LUN for a copy of the metadata. These blocks are not exposed to the host initiator. When a host reads the capacity of the LUN, the size reported is always three block less than the actual size. The behavior is enforced by selecting the **New LUN** checkbox on the **Select LUN** screen of the **Add New Path** wizard when adding the LUNs for an SRDF pair (e.g., R1 and R2 in [Figure 248](#)).

Not the following when using the **New LUN** option:

- Both LUNs that form a SRDF pair must be added to their containers using the **New LUN** option.
- At any site all paths to a given SRDF device must be configured with the **New LUN** option.
- All LUNs configured with the **New LUN** option will report 3 blocks less than the actual size when host performs READ CAPACITY 10/READ CAPACITY 16.
- If a LUN is added with the **New LUN** option and with encryption enabled, it will always have valid metadata even if block 1-16 of the LUN is not compressible.
- LUNs configured as cleartext must also be added with the **New LUN** option if part of a SRDF pair. This is to handle scenarios where the LUN policy is changed to encrypted at some later time, and to verify formation of DEK clusters and LUN accessibility prior to enabling encryption for the LUN. When cleartext LUNs are configured with the **New LUN** option, no metadata is written to the last 3 blocks, but will still report 3 blocks less than the actual size when host performs READ CAPACITY 10/READ CAPACITY 16.

- The **New LUN** option is used only if an RKM key vault is configured for the encryption group.
- The **New LUN** option can be used only if replication is enabled for the encryption group.
- If the local LUN contains host data, configuring it with the **New LUN** option would cause the data on the last 3 blocks of the LUN to be lost. Before using the **New LUN** option, you must migrate the contents of the LUN to another LUN that is larger by at least 3 blocks. The new larger LUN can then be used when creating the SRDF pair. The remote LUN of the SRDF pair must be of the same size. The original smaller LUN with user data can be decommissioned.

## Adding Target Tape LUNs for encryption

You configure a Crypto LUN by adding the LUN to the CryptoTarget container and enabling the encryption property on the Crypto LUN. You must add LUNs manually. After you add the LUNs, you must specify the encryption settings.

When configuring a LUN with multiple paths, the same LUN policies must be configured on all the LUN's paths. If there are multiple paths to the same physical LUNs, then the LUNs are added to multiple target containers (one target per storage device port). See [“Configuring encrypted tape storage in a multi-path environment”](#) on page 557 for a multi-path configuration scenario.

1. Select **Configure > Encryption** from the menu bar.

The **Encryption Center** dialog box displays.

2. Select the encryption group, switch, or encryption engine containing the storage device to be configured.
3. Click **Encryption Targets**.

The **Encryption Targets** dialog box displays.

4. Select a Target storage device from the list, and click **LUNs**.

The **Encryption Target LUNs** dialog box displays.

5. Click **Add**.

The **Add Encryption Target Tape LUNs** dialog box displays.

This dialog box includes a table of all LUNs in the storage device that are visible to hosts. LUNs are identified by the Host world wide name, LUN number, and Volume Label Prefix number.

6. Select a host from the **Host** list.

Before you encrypt a LUN you must select a host and then either discover LUNs that are visible to the virtual initiator representing the selected host, or enter a range of LUN numbers to be configured for the selected host.

7. Choose a LUN to be added to an encryption target container using one of the two following methods:
  - **Discover.** Click to identify the exposed logical unit number for a specified initiator. If you already know the exposed LUNs for the various initiators accessing the LUN, you can enter the range of LUNs using the alternative method.
  - **Enter a LUN number range.** Click to add a range of LUNs to be configured for the selected host. The LUN needed for configuring a Crypto LUN is the LUN that is exposed to a particular initiator.

8. Select the desired encryption mode.
  - If you change a LUN policy from **Native Encryption** or **DF-Compatible Encryption** to **Clear Text**, you disable encryption.
  - The LUNs of the target which are not enabled for encryption must still be added to the CryptoTarget container with the **Clear Text** encryption mode option.

**NOTE**

The Re-keying interval can only be changed for disk LUNs. For tape LUNs, expiration of the re-keying interval simply triggers the generation of a new key, to be used on future tape volumes. Tapes that are already made are not re-keyed. To re-key a tape, you would need to read the tape contents using a host application that decrypts the tape contents using the old key, and then re-write the tape, which re-encrypts the data with the new key.

9. Click **OK**.

The selected tape LUNs are added to the encryption target container.

## Configuring encrypted tape storage in a multi-path environment

This example assumes one host accessing one storage device using two paths:

- The first path is from host port A to target port A, using encryption engine A for encryption.
- The second path is from host port B to target port B, using encryption engine B for encryption.

Encryption engines A and B are in switches that are already part of encryption group X.

The following is the procedure for configuring this scenario using the Management application.

1. Zone host port A and target port A, using the **Configure > Zoning** dialog box.
2. Zone host port B and target port B, using the **Configure > Zoning** dialog box.
3. Open the **Encryption Center** dialog box by selecting **Configure > Encryption** from the Management application's main menu.
4. Click the **View By Encryption Groups** button to display the encryption groups.
5. Select encryption group X, then click the **Encryption Targets** button.
6. Click the **Add** button to start the **Configure Storage Encryption** wizard. Use the **Configure Storage Encryption** wizard to create a target container for encryption engine A with target port A and host port A.
7. Run the **Configure Storage Encryption** wizard again to create a target container for encryption engine B with target port B and host port B.

Up to this point, the Management application has been automatically committing changes as they are made. The targets and hosts are now fully configured; only the LUN configuration remains.

8. In the **Encryption Targets** dialog box, select target port A, click **LUNs**, then click **Add**. Select the LUNs to be encrypted and the encryption policies for the LUNs.

9. Select target port B, click **LUNs**, then click **Add**. Select the LUNs to be encrypted and the encryption policies for the LUNs, making sure that the encryption policies match the policies specified in the other path.
10. Click **Commit** to make the LUN configuration changes effective in both paths simultaneously.

The Management application does not automatically commit LUN configuration changes. This allows matching changes made in a multi-path environment to be committed together, preventing cases where one path may be encrypting and another path is not encrypting, resulting in corrupted data. You must remember to click the **Commit** button after any LUN configuration changes, even in non-multi-path environments. The **Encryption Targets** dialog box displays a reminder if you attempt to close the dialog box without committing LUN configuration changes.

---

#### NOTE

There is a limit of 25 uncommitted LUN configuration changes. When adding more than 12 LUNs in a multi-path environment, repeat steps [step 8](#) through [step 10](#) above, adding only 12 LUNs to each target container at a time. Each commit operation, then, will commit 24 LUNs, 12 in each path.

---

## Re-balancing the encryption engine

If you are currently using encryption and running Fabric OS version 6.3.x or earlier, you are hosting tape and disk target containers on different encryption switches or blades. Beginning with Fabric OS version 6.4, disk and tape target containers can be hosted on the same switch or blade. Hosting both disk and tape target containers on the same switch or blade may result in a drop in throughput, but it can reduce cost by reducing the number of switches or blades needed to support encrypted I/O in environments that use both disk and tape.

The throughput drop can be mitigated by re-balancing the tape and disk target containers across the encryption engine. This ensures that the tape and disk target containers are distributed within the encryption engine for maximum throughput.

All nodes within an encryption group must be upgraded to Fabric OS version 6.4 or a later release to support hosting disk and tape target containers on the same encryption engine. If any node within an encryption group is running an earlier release, disk and tape containers must continue to be hosted on separate encryption engines.

During re-balancing operations, be aware of the following:

- You may notice a slight disruption in Disk I/O. In some cases, manual intervention may be needed.
- Backup jobs to tapes may need to be restarted after re-balancing completes.

To determine if re-balancing is recommended for an encryption engine, check the encryption engine properties. Beginning with Fabric OS version 6.4, a field is added that indicates whether or not re-balancing is recommended

You may be prompted to rebalance during the following operations:

- When adding a new disk or tape target container.
- When removing an existing disk or tape target container.
- After failover to a backup encryption engine in an HA cluster.
- After an failed encryption engine in an HA cluster is recovered, and failback processing has taken place.

To rebalance an encryption engine, do the following.

1. Select **Configure > Encryption** from the menu bar.

The **Encryption Center** dialog box displays.

2. Select an encryption engine and select **Engine > Re-Balance** from the menu bar, or right click on the encryption engine, and select **Re-Balance**.

A warning message displays, cautioning you about the potential disruption of disk and tape I/O, and telling you that the operation may take several minutes.

3. Click **Yes** to begin re-balancing.

## Master keys

When an opaque key vault is used, a master key is used to encrypt the data encryption keys. The master key status indicates whether a master key is used and whether it has been backed up. Encryption is not allowed until the master key has been backed up.

Only the active master key can be backed up, and multiple backups are recommended. You can back up or restore the master key to the key vault, to a file, or to a recovery card set. A recovery card set is set of smart cards. Each recovery card holds a portion of the master key. The cards must be gathered and read together from a card reader attached to a PC running the Management application to restore the master key.

---

### NOTE

It is very important to back up the master key because if the master key is lost, none of the data encryption keys can be restored and none of the encrypted data can be decrypted.

---

## Active master key

The active master key is used to encrypt newly-created data encryption keys (DEKs) prior to sending them to a key vault to be stored. You can restore the active master key under the following conditions:

- The active master key has been lost, which happens if all encryption engines in the group have been zeroized or replaced with new hardware at the same time.
- You want multiple encryption groups to share the same active master key. Groups should share the same master key if the groups share the same key vault and tapes (or disks) are going to be regularly exchanged between the groups.

## Alternate master key

The alternate master key is used to decrypt data encryption keys that were not encrypted with the active master key. Restore the alternate master key for the following reasons:

- To read an old tape that was created when the group used a different active master key.
- To read a tape (or disk) from a different encryption group that uses a different active master key.

## Master key actions

Master key actions are as follows:

- **Backup master key**, which is enabled any time a master key exists.
- **Restore master key**, which is enabled when no master key exists or the previous master key has been backed up.
- **Create new master key**, which is enabled when no master key exists or the previous master key has been backed up.

## Reasons master keys can be disabled

Master key actions are disabled if unavailable. There are several ways a master key can be disabled:

- The user does not have Storage Encryption Security permissions. See [“Encryption user privileges”](#) on page 495 for more information.
- The group leader is not discovered or managed by the Management application.

## Saving the master key to a file

Use the following procedure to save the master key to a file.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Select an encryption group from the tree, and click **Properties**.

---

**NOTE**

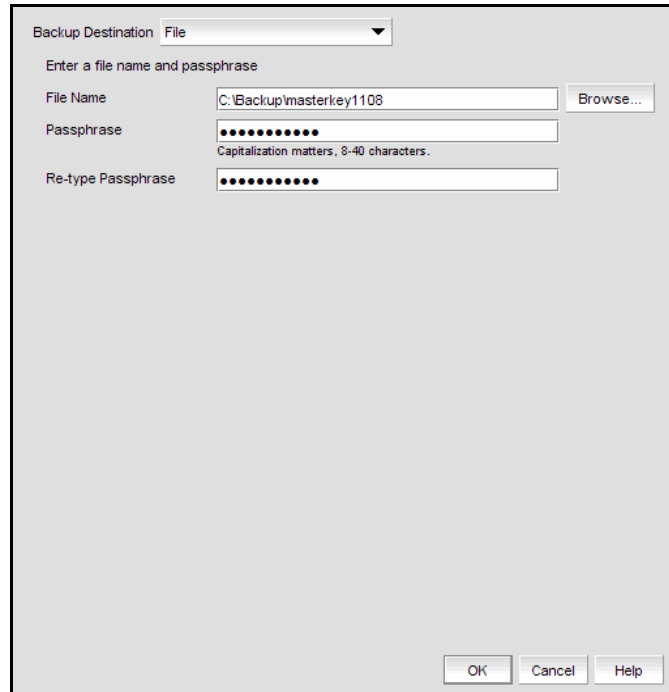
Master keys belong to the group and are managed from the group properties.

---

3. Select the **Security** tab.

4. Select **Backup Master Key** as the **Master Key Action**.

The **Master Key Backup** dialog box displays, but only if the master key has already been generated.



**FIGURE 249** Backup Destination (to file) dialog box

5. Select **File** as the **Backup Destination**.
6. Enter a file name, or browse to the desired location.
7. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
8. Re-type the passphrase for verification.
9. Click **OK**.

---

**ATTENTION**

Save the passphrase. This passphrase is required if you ever need to restore the master key from the file.

---

## Saving a master key to a key vault

Use the following procedure to save the master key to a key vault.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Backup Master Key** as the **Master Key Action**.

The **Backup Master Key for Encryption Group** dialog box displays.

Backup Destination: Key Vault

Enter a Passphrase

Passphrase: [Redacted]

Re-type Passphrase: [Redacted]

Capitalization matters, 8-40 characters.

OK Cancel Help

**FIGURE 250** Backup Destination (to key vault) dialog box

5. Select **Key Vault** as the **Backup Destination**.
6. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
7. Re-type the passphrase for verification.
8. Click **OK**.  
A dialog box displays that shows the **Key ID**.
9. Store both the **Key ID** and the passphrase in a secure place. Both will be required to restore the master key in the future. (The **Key ID** identifies the storage location in the key vault.)
10. Click **OK** after you have copied the key ID.

## Saving a master key to a smart card set

A card reader must be attached to the SAN Management application PC to complete this procedure. Recovery cards can only be written once to back up a single master key. Each master key backup operation requires a new set of previously unused smart cards.

---

### NOTE

Windows operating systems do not require smart card drivers to be installed separately; the driver is bundled with the operating system. You must install a smart card driver for Linux and Solaris operating systems, however. For instructions, see the *Data Center Fabric Manager Administrator's Guide*.

---

The key is divided between the cards in the card set. When the master key is backed up to a set of three cards, a minimum of two cards can be used together to restore the master key. When the master key is backed up to a set of five cards, a minimum of three cards can be used together to restore the master key. Backing up the master key to multiple recovery cards is the recommended and most secure option.

---

### NOTE

When you write the key to the card set, be sure you write the full set without canceling. If you cancel, all the previously written cards become unusable, and you will need to discard them and create a new set.

---

1. Select **Configure > Encryption** from the menu bar.

The **Encryption Center** dialog box displays.

2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Backup Master Key** as the **Master Key Action**.

The **Backup Master Key for Encryption Group** dialog box displays.

FIGURE 251 Backup Destination (to smart cards) dialog box

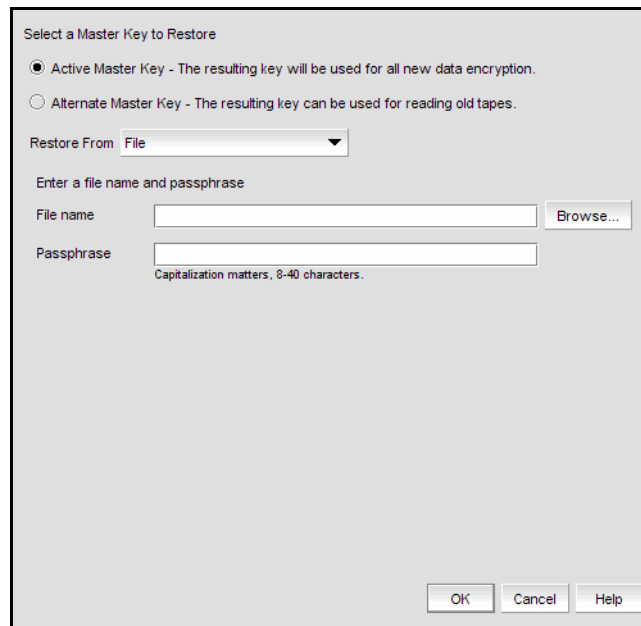
5. Select **A Recovery Set of Smart Cards** as the **Backup Destination**.
6. Enter the recovery card set size.
7. Insert the first blank card and wait for the card serial number to appear.
8. Run the additional cards needed for the set through the reader. As you read each card, the card ID displays in the **Card Serial#** field. Be sure to wait for the ID to appear.
9. Enter the mandatory last name and first name of the person to whom the card is assigned.
10. Type a Card **Password**.
11. Re-type the password for verification.
12. Record and store the password in a secure location.
13. Click **Write Card**.  
The dialog box prompts you to insert the next card, up to the number of cards specified in [step 6](#).
14. Repeat [step 7](#) through [step 13](#) for each card.
15. Continue until you have written to all the cards in the set.
16. After the last card is written, click **OK** in the **Master Key Backup** dialog box to finish the operation.

## Restoring a master key from a file

Use the following procedure to restore the master key from a file.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Restore Master Key** as the **Master Key Action**.

The **Restore Master Key for Encryption Group** dialog box displays.



**FIGURE 252** Select a Master Key to Restore (from file) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to [“Active master key”](#) on page 559 and [“Alternate master key”](#) on page 559 if you need more information on active and alternate master keys.
6. Select **File** as the **Restore From** location.
7. Enter a file name, or browse to the desired location.
8. Enter the passphrase. The passphrase that was used to back up the master key must be used to restore the master key.
9. Click **OK**.

## Restoring a master key from a key vault

Use the following procedure to restore the master key from a key vault.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Restore Master Key** as the **Master Key Action**.

The **Restore Master Key for Encryption Group** dialog box displays.

Select a Master Key to Restore

☒ Active Master Key - The resulting key will be used for all new data encryption.

☐ Alternate Master Key - The resulting key can be used for reading old tapes.

Restore From: Key Vault

Key ID:

Enter a passphrase to decrypt the master key

Passphrase:

Capitalization matters, 8-40 characters.

OK Cancel Help

**FIGURE 253** Select a Master Key to Restore (from key vault) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to [“Active master key”](#) on page 559 and [“Alternate master key”](#) on page 559 if you need more information on active and alternate master keys.
6. Select **Key Vault** as the **Restore From** location.
7. Enter the key ID of the master key that was backed up to the key vault.
8. Enter the passphrase. The passphrase that was used to back up the master key must be used to restore the master key.
9. Click **OK**.

## Restoring a master key from a smart card set

A card reader must be attached to the SAN Management application PC to complete this procedure.

Use the following procedure to restore the master key from a set of smart cards.

1. Select **Configure > Encryption** from the menu bar.

The **Encryption Center** dialog box displays.

2. Select an encryption group from the tree, and click **Properties**.
3. Select the **Security** tab.
4. Select **Restore Master Key** as the **Master Key Action**.

The **Restore Master Key for Encryption Group** dialog box displays.

Select a Master Key to Restore

☒ Active Master Key - The resulting key will be used for all new data encryption.

☐ Alternate Master Key - The resulting key can be used for reading old tapes.

Restore From: A Recovery Set of Smart Cards ▼

You will need a card reader attached to the management station and recovery cards.

1) Insert each card, in turn, into the card reader and wait for its ID to appear below.

Card ID:

2) Enter card password below.

Card Password:  Capitalization matters.

3)

| Completed | Card | Card ID | First Name | Last Name | Notes |
|-----------|------|---------|------------|-----------|-------|
|           |      |         |            |           |       |

Status: Waiting for card to be inserted ...

**FIGURE 254** Select a Master Key to Restore (from a recovery set of smart cards) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to [“Active master key”](#) on page 559 and [“Alternate master key”](#) on page 559 if you need more information on active and alternate master keys.
6. Select **A Recovery Set of Smart Cards** as the **Restore From** location.
7. Insert the recovery card containing a share of the master key that was backed up earlier, and wait for the card serial number to appear.
8. Enter the password that was used to create the card. After five unsuccessful attempts to enter the correct password, the card becomes locked and unusable.
9. Click **Restore**.

The dialog box prompts you to insert the next card, if needed.

10. Insert the next card, and repeat [step 8](#) and [step 9](#).
11. Continue until all the cards in the set have been read.
12. Click **OK**.

## Creating a new master key

Though it is generally not necessary to create a new master key, you may be required to create one due to circumstances such as the following:

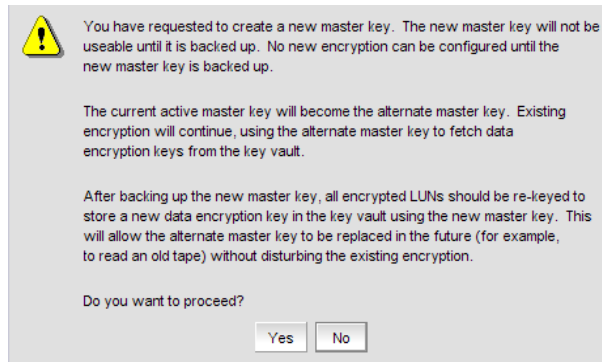
- The previous master key has been compromised.
- Corporate policy might require a new master key every year for security purposes.

When you create a new master key, the former active master key automatically becomes the alternate master key.

The new master key cannot be used (no new data encryption keys can be created, so no new encrypted LUNs can be configured), until you back up the new master key. After you have backed up the new master key, it is strongly recommended that all encrypted disk LUNs be re-keyed. Re-keying causes a new data encryption key to be created and encrypted using the new active master key, thereby removing any dependency on the old master key.

1. Select **Configure > Encryption**.
2. Select an encryption group from the tree and click **Properties**.
3. Select the **Security** tab.
4. Select **Create a New Master Key** from the list.

The **Confirm Master Key Creation** dialog box displays.



**FIGURE 255** Confirm master key creation dialog box

5. Read the information, and click **Yes** to proceed.

## Zeroizing an encryption engine

Zeroizing is the process of erasing all data encryption keys and other sensitive encryption information in an encryption engine. You can zeroize an encryption engine manually to protect encryption keys. No data is lost because the data encryption keys for the encryption targets are stored in the key vault.

Zeroizing has the following effects:

- All copies of data encryption keys kept in the encryption switch or encryption blade are erased.
- Internal public and private key pairs that identify the encryption engine are erased and the encryption switch or the encryption blade is in the FAULTY state.
- All encryption operations on this engine are stopped and all virtual initiators (VI) and virtual targets (VT) are removed from the fabric's name service.
- The key vault link key (for NetApp LKM key vaults) or the master key (for other key vaults) is erased from the encryption engine.

Once enabled, the encryption engine is able to restore the necessary data encryption keys from the key vault when the link key (for the NetApp Lifetime Key Management application) or the master key (for other key vaults) are restored.

- If the encryption engine was part of an HA cluster, targets fail over to the peer which assumes the encryption of all storage targets. Data flow will continue to be encrypted.
- If there is no HA backup, host traffic to the target will fail as if the target has gone offline. The host will not have unencrypted access to the target. There will be no data flow at all because the encryption virtual targets will be offline.

---

### NOTE

Zeroizing an engine affects the I/Os but all target and LUN configuration is intact. Encryption target configuration data is not deleted.

---

You can zeroize an encryption engine only if it is enabled (running) or disabled, but ready to be enabled. If the encryption engine is not in one of these states, an error message displays.

When using a NetApp LKM key vault, if all the encryption engines in a switch are zeroized, the switch loses the link key required to communicate with the LKM vault. After the encryption engines are rebooted and re-enabled, you must use the CLI to create new link keys for the switch.

When using an opaque key vault, if all the encryption engines in an encryption group are zeroized, the encryption group loses the master key required to read data encryption keys from the key vault. After the encryption engines are rebooted and re-enabled, you must restore the master key from a backup copy, or alternatively you can also generate a new master key and back it up. Restoring the master key from a backup copy or generating a new master key and backing it up indicates that all previously generated DEKs will not be decryptable, unless the original master key used to encrypt them is restored.

Use the **Restore Master key** wizard from the **Encryption Group Properties** dialog box to restore the master key from a backup copy.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Select the encryption engine.
3. Right-click, or select **Engine** from the menu bar, and select **Zeroize**.

A confirmation dialog box describing consequences and actions required to recover launches.



- 4. Click **YES** to zeroize the encryption engine.

## Encryption Targets dialog box

The **Encryption Targets** dialog box enables you to send outbound data that you want to store as ciphertext to an encryption device. The encryption target acts as a virtual target when receiving data from a host, and as a virtual initiator when writing the encrypted data to storage.

To access the Encryption Targets dialog box, complete the following steps.

- 1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays, showing the status of all encryption-related hardware and functions.
- 2. Select the **Group >Targets**, **Switch > Targets**, or **Engine > Targets**, from the tool bar menu, or right-click on the group, switch, or encryption engine in the **Encryption Devices** table, and select **Targets**.

The **Encryption Targets** dialog box (Figure 256) displays the targets currently being encrypted by the selected group, switch, or encryption engine. If a group is selected, all configured targets in the group are displayed. If a switch is selected, all configured targets for the switch are displayed.

The **Encryption Targets** dialog box enables you to launch a variety of wizards and other related dialog boxes, which are defined in Table 24.

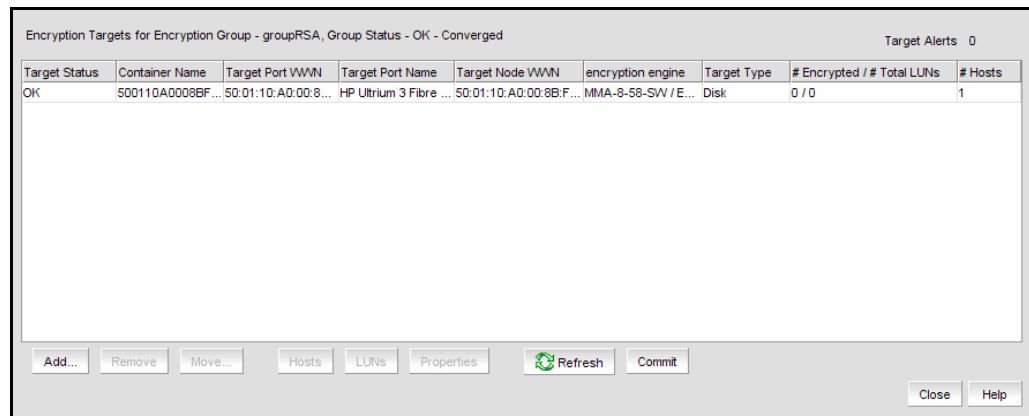



FIGURE 256 Encryption Targets dialog box

TABLE 24 Encryption Targets dialog box fields and components

| Feature              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Add button</b>    | <p>Launches the <b>Storage Encryption Setup Wizard</b>, which enables you to configure a new target for encryption. It is the first step in configuring encryption for a storage device.</p> <p>It is recommended that you zone the host and target together before you add container information.</p> <ul style="list-style-type: none"> <li><b>Note:</b> If the group is in <b>OK-Converged</b> mode, the group leader can communicate with all members. The <b>Configure Storage Encryption</b> wizard dialog box launches when you click <b>Add</b>.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>If a group is in the <b>Degraded</b> state, the following operations are not allowed: key vault changes, master key operations, enable/disable encryption engines, failback mode changes, HA Cluster creation or addition (removal is allowed), tape pool changes, and any configuration changes for storage targets, hosts, and LUNs.</li> <li>If a group is in the <b>Unknown</b> state, the group leader is in an unmanaged fabric.</li> </ul> |
| <b>Remove button</b> | <p>Removes a selected target. Proceed only if the data on the LUN is to be disabled or if the LUN is to be configured for encryption again on some other encryption engine. If the LUN data is to be enabled and later accessed by way of another encryption engine, you should unzone the host with the encryption engine <i>before</i> you remove the encryption target from the encryption engine. This prevents the host from accidentally writing to the encryption target during the unencrypted interim period.</p> <div style="text-align: center;">  </div> <p><b>CAUTION</b></p> <p>Removing a selected target can result in data loss, if the host is writing to the target as it is removed. Removing the target will result in lost access to the data, but the data remains encrypted on the target.</p>                                                                                                                                                                       |
| <b>Move button</b>   | <p>Moves one encryption target to a different encryption engine. The target and engine must be in the same encryption group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**TABLE 24** Encryption Targets dialog box fields and components (Continued)

| Feature                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hosts</b> button      | Launches the <b>Encryption Target Hosts</b> dialog box, where you can configure hosts to access the selected encryption target.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>LUNs</b> button       | Launches the <b>Encryption Target LUNs</b> dialog box, where you can display existing LUNs and add new LUNs. The button is enabled only if there are hosts associated with the targets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Commit</b> button     | Commits LUN changes, including adding, removing, or modifying disk or tape LUNs.<br>If there are multiple paths to the same physical LUNs, then the LUNs are added to multiple target containers (one target per storage device port). When adding, modifying, or removing multi-pathed LUNs, make the same changes in all target containers, and then click Commit to apply all the changes at once. This keeps the LUN settings consistent on each path.<br>There is a limit of 25 LUN changes, including adding, modifying, or removing LUNs, per Commit operation.<br><b>Note:</b> The <b>Commit</b> button can also be used to re-create any redirection zones that were accidentally modified or removed. |
| <b>Abort</b> button      | Aborts all transactions that have been configured but are not yet committed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Properties</b> button | Launches the <b>Encryption Target Properties</b> dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Refresh</b> button    | Refreshes the displayed data from the database maintained on the server. It does not collect new information from the hardware switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Redirection zones

It is recommended that you zone the host and target together before configuring them for encryption. Configuring a host/target pair for encryption normally creates a re-direction zone to redirect the host-target traffic through the encryption engine. But redirection zones can only be created if the host and target are already zoned. If the host and target are not already zoned, you can still configure them for encryption, but afterward you will need to zone the host and target together, and then click the **Commit** button to create the re-direction zones as a separate step.

### NOTE

If you click the **Commit** button and the encryption group is busy, you are given the option to force the commit or abort the changes. Click the **Commit** button to re-create the redirection zones.

## Disk device decommissioning

A disk device needs to be decommissioned when any of the following occur:

- The storage lease expires for an array, and devices must be returned or exchanged.
- Storage is reprovisioned for movement between departments.
- An array or device is removed from service.

In all cases, all data on the disk media must be rendered inaccessible. Device decommissioning deletes all information that could be used to recover the data.

When a device decommission operation fails on the encryption group leader for any reason, the crypto configuration remains uncommitted until a user-initiated commit or a subsequent device decommission operation issued on the encryption group leader completes successfully. Device decommission operations should always be issued from a committed configuration. If not, the operation will fail with the error message **An outstanding transaction is pending in Switch/EG**. If this happens, you can resolve the problems by committing the configuration from the encryption group leader.

Provided that the crypto configuration is not left uncommitted because of any crypto configuration changes or a failed device decommission operation issued on an encryption group leader node, this error message will not be seen for any device decommission operation issued serially on an encryption group member node. If more than one device decommission operation is tried in an encryption group from member nodes simultaneously, then this error message is transient and will go away after device decommission operation is complete. If the device decommissioning operation fails, retry the operation after some time has passed.

### Decommissioning LUNs

Use the following procedure to decommission a LUN.

1. Select **Configure > Encryption** from the menu bar.

The **Encryption Center** dialog box displays.

2. Select the encryption group, switch, or encryption engine containing the storage device or devices to be decommissioned.

3. Select **Encryption Targets**.

The **Encryption Targets** dialog box displays.

4. Select a Target storage device from the list, and click **LUNs**.

The **Encryption Target LUNs** dialog box displays.

5. Select the LUNs associated with the device, and click the **Decommission** button.

A Warning message displays.

6. Click **Yes** to proceed with decommissioning.

If a re-key operation is currently in progress on a selected LUN, a message is displayed that gives you a choice of doing a **Forced Decommission**, or to **Cancel** and try later after the re-key operation is complete.

7. To check on the progress of the decommissioning operation, click Refresh. When decommissioning is complete, the LUNs are removed from the **Encryption Target LUNs** dialog box.

## Displaying and deleting decommissioned key IDs

When disk LUNs are decommissioned, the process includes the disabling of the key record in the key vault and indicating that the key has been decommissioned. These decommissioned keys are still stored on the switch. You can display them, copy them, and delete them as an additional security measure.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays.
2. Right click on the switch, and select **Decommissioned keyids**.  
The **Decommissioned Key IDs** dialog box displays.
3. Click **Delete All** to delete the decommissioned keys from the switch. As a precaution, you may want to copy the keys to a secure location before deleting them from the switch. To export the keys, right-click and select **Export** which will export all the key IDs.

## Viewing and editing switch encryption properties

To view switch encryption properties, complete the following steps.

1. Select **Configure > Encryption** from the menu bar.  
The **Encryption Center** dialog box displays the status of all encryption-related hardware and functions at a glance. It is the single launching point for all encryption-related configuration.
2. Select the switch or encryption engine from the **Encryption Devices** table, and select **Switch > Properties** or **Engine > Properties** from the menu bar, or right-click the switch or encryption engine and select **Properties**.  
The **Encryption Properties** dialog box, shown in [Figure 257](#), contains the following information:

[illegible]

**FIGURE 257** Encryption Properties dialog box

- **Switch Properties** table - the properties associated with the selected switch.
- **Name** - the name of the selected switch.
- **Node WWN** - the world wide name of the node.
- **Switch Status** - the health status of the switch. Possible values are Healthy, Marginal, Down, Unknown, Unmonitored, and Unreachable.
- **Switch Membership Status** - the alert or informational message description which details the health status of the switch. Possible values are Group Member, Leader-Member Comm, Error, Discovering, and Not a member.
- **Encryption Group** - the name of the encryption group to which the switch belongs.
- **Encryption Group Status** - Possible values are:
  - **OK - Converged** - the group leader can communicate with all members.
  - **Degraded** - the group leader cannot communicate with one or more members.
  - **Unknown** - the group leader is in an unmanaged fabric.

## NOTE

**Note** When a group is in the **Degraded** state, the following operations are not allowed: key vault changes, master key operations, enable/disable encryption engines, Failback mode changes, HA Cluster creation or addition (removal is allowed), and any configuration changes for storage targets, hosts, and LUNs.

- **Fabric** - the name of the fabric to which the switch belongs.

- **Domain ID** - the domain ID of the selected switch.
- **Firmware Version** - the current encryption firmware on the switch.
- **Primary Key Vault Link Key Status** - the possible statuses are as follows:
  - **Not Used** - the key vault type is not LKM.
  - **No Link Key** - no access request was sent to an LKM yet, or a previous request was not accepted.
  - **Waiting for LKM approval** - a request was sent to LKM and is waiting for the LKM administrator's approval.
  - **Waiting for local approval** - a response was received from LKM.
  - **Created, not validated** - the interim state until first used.
  - **OK** - a shared link key exists and has been successfully used.
- **Primary Key Vault Connection Status** - whether the primary key vault link is connected. Possible values are Unknown, Key Vault Not Configured, No Response, Failed authentication, and Connected.
- **Backup Key Vault Link Key Status** - the possible statuses are as follows:
  - **Not Used** - the key vault type is not LKM.
  - **No Link Key** - no access request was sent to an LKM yet, or a previous request was not accepted.
  - **Waiting for LKM approval** - a request was sent to LKM and is waiting for the LKM administrator's approval.
  - **Waiting for local approval** - a response was received from LKM.
  - **Created, not validated** - the interim state until first used.
  - **OK** - a shared link key exists and has been successfully used.
- **Backup Key Vault Connection Status** - whether the backup key vault link is connected. Possible values are Unknown, Key Vault Not Configured, No Response, Failed authentication, and Connected.
- **Public Key Certificate** text box - the switch's KAC certificate, which must be installed on the primary and backup key vaults.
- **Save As** button - saves the certificate to a file in PEM format. The file may be loaded into the key vault using the key vault's tools.
- **Encryption Engine Properties** table - the properties for the encryption engine. There may be 0 to 4 slots, one for each encryption engine in the switch.
- **Current Status** - the status of the encryption engine. There are many possible values, but common values are Not Available (the engine is not initialized), Disabled, Operational, need master/link key, and Online.
- **Set State To** - enter a new value, enabled or disabled, and click OK to apply the change.
- **Total Targets** - the number of the encrypted target device.
- **HA Cluster Peer** - the name and location of the high-availability (HA) cluster peer (another encryption engine in the same group), if in an HA configuration.

- **HA Cluster Name** - the name of the HA cluster (for example, Cluster1), if in an HA configuration. The name can have a maximum of 31 characters. Only letters, digits, and underscores are allowed.
- **Media Type** - the media type of the encryption engine. Possible values are Disk and Tape.
- **Re-Balance Recommended** - A value of **Yes** or **No** indicating whether or not LUN re-balancing is recommended for an encryption engine that is hosting both disk and tape LUNs.
- **System Card** - the current status of system card information for the encryption engine. (registered or not registered).

## Exporting the public key certificate signing request (CSR) from Properties

To export the CSR under Public Key Certificate Request, complete the following steps.

1. Click **Export**.

A **Save** dialog box displays.

2. Browse to the location where you want to save the certificate.
3. Click **Save**.

Alternatively, you may also copy the CSR and paste it to a file.

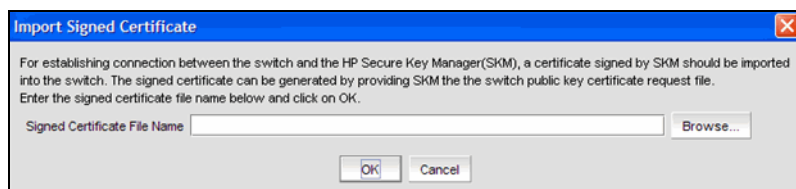
4. Submit the CSR to a certificate authority (CA) for signing. CA signing requirements and procedures differ per key manager appliance. Refer to [“Supported encryption key manager appliances”](#) on page 504 and look through the following sections to find the procedure that applies.

## Importing a signed public key certificate from Properties

To import a signed public key certificate, complete the following steps.

1. Click **Import**.

The Import Signed Certificate dialog box displays.



2. Enter or browse to the file containing the signed certificate.
3. Click **OK**.

The file is imported onto the switch.

## Enabling the encryption engine state from Properties

To enable the encryption engine, complete the following steps.

1. Find the **Set State To** entry under **Encryption Engine Properties**.
2. Click the field and select **Enabled**.
3. Click **OK**.

## Disabling the encryption engine state from Properties

To disable the encryption engine, complete the following steps.

1. Find the **Set State To** entry under **Encryption Engine Properties**.
2. Click the field and select **Disabled**.
3. Click **OK**.

## Viewing and editing group properties

To view encryption group properties, complete the following steps.

1. Select **Configure > Encryption**.

The **Encryption Center** dialog box displays.

2. If groups are not visible in the **Encryption Devices** table, select **View > Groups** from the menu bar.

The encryption groups display in the **Encryption Devices** table.

3. Select a group from the **Encryption Devices** table, and select **Group > Properties** from the menu bar, or right-click the group and select **Properties**.

The **Encryption Group Properties** dialog box, shown in [Figure 257](#), has six tabs which are defined in this section:

- [“General tab”](#) on page 579
- [“Members tab”](#) on page 580
- [“Security tab”](#) on page 583
- [“HA Clusters tab”](#) on page 584
- [“Engine Operations tab”](#) on page 584
- [“Link Keys tab”](#) on page 585
- [“Tape Pools tab”](#) on page 585

---

### NOTE

The **Link Keys** tab appears only if the key vault type is NetApp LKM.

---

General Members Security HA Clusters Tape Pools Engine Operations

groupabc

|                                                 |                             |
|-------------------------------------------------|-----------------------------|
| Encryption Group Name                           | groupabc                    |
| Group Status                                    | OK - Converged              |
| Deployment Mode                                 | Transparent                 |
| Failback Mode                                   | Automatic                   |
| Key Vault Type                                  | HP Secure Key Manager (SKM) |
| Primary Key Vault IP Address (IPv4 or hostname) | 10.32.45.13                 |
| Backup Key Vault IP Address (IPv4 or hostname)  | None                        |

If you specify a key vault IP address above, then you must enter a key vault certificate below.  
If a key vault address is not specified above, then entries below are ignored.

Primary Key Vault Certificate

Version: V3  
Subject: EMAILADDRESS=support@brocade.com, CN=maceftv, OU=Data Security, O=Data Security, L=Brocade, ST=CA, C=US  
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5  
Key: RSA public key, 2048 bits

Load from File...

Backup Key Vault Certificate

<None>

Load from File...

OK Cancel Help

**FIGURE 258** Encryption Group Properties dialog box

## General tab

The properties displayed in the **General** tab are described below.

- **Encryption group name** - the name of the encryption group.
- **Group status** - the status of the encryption group, which can be **OK-Converged** or **Degraded**. Degraded means the group leader cannot contact all of the configured group members.
- **Deployment mode** - the group's deployment mode, which is transparent.
- **Failback mode** - The group's failback mode, which can be automatic or manual. The failback mode can be changed by clicking on the field and selecting the desired mode.
- **Key vault** - the vault type, either RSA Key Manager (RKM) NetApp Lifetime Key Manager (LKM), HP Secure Key Manager (SKM), Thales Encryption Manager for Storage (TEMS), or Tivoli Key Lifetime Manager (TKLM).
- **REPL Support** - whether or not remote replication LUNs support is enabled or disabled. You can change the current setting by clicking on the field and selecting the desired state.
- **Primary Key Vault IP address** - The IP address of the primary key vault, either IPv4 or host name.
- **Primary Key Vault Connection Status** - the status of the connection to the primary key vault. In an operating environment, the status should be Connected.
- **Backup key vault IP address** - the IP address of the backup key vault.
- **Backup Key Vault Connection Status** - the status of the connection to the backup key vault, if a backup is configured.
- **Primary key vault certificate** - the details of the primary vault certificate; for example, version and signature information.
- **Backup key vault certificate** - the details of the backup vault certificate; for example, version and signature information.

## Members tab

The **Group Members** tab lists group switches, their role, and their connection status with the group leader. The tab displays the configured membership for the group (none of the table columns are editable). The list can be different from the members displayed in the **Encryption Center** dialog box if some configured members are unmanaged, missing, or in a different group.

Possible **Connection Status** values are as follows:

- **Group Leader** - this switch is the group leader so there is no connection status.
- **Trying to Contact** - the member is not responding to the group leader. This may occur if the member switch is not reachable by way of the management port, or if the member switch does not believe it is part of the encryption group.
- **Configuring** - the member switch has responded and the group leader is exchanging information. This is a transient condition that exists for a short time after a switch is added or restored to a group.
- **OK** - the member switch is responding to the group leader switch.
- **Not Available** - the group leader is not a managed switch, so connection statuses are not being collected from the group leader.

### *Members tab Remove button*

You can click the **Remove** button to remove a selected switch or an encryption group from the encryption group table.

- You cannot remove the group leader unless it is the only switch in the group. If you remove the group leader, the Management application also removes the HA cluster, the target container, and the tape pool (if configured) that are associated with the switch.
- If you remove a switch from an encryption group, the Management application also removes the HA cluster and target container associated with the switch.

---

#### **NOTE**

If the encryption group is in a degraded state, the Management application does not remove the HA clusters or target containers associated with the switch. In this case, a pop-up error message displays.

---

- If you remove the last switch from a group, the Management application also deletes the group.

## Consequences of removing an encryption switch

Table 25 explains the impact of removing switches.

**TABLE 25** Switch removal impact


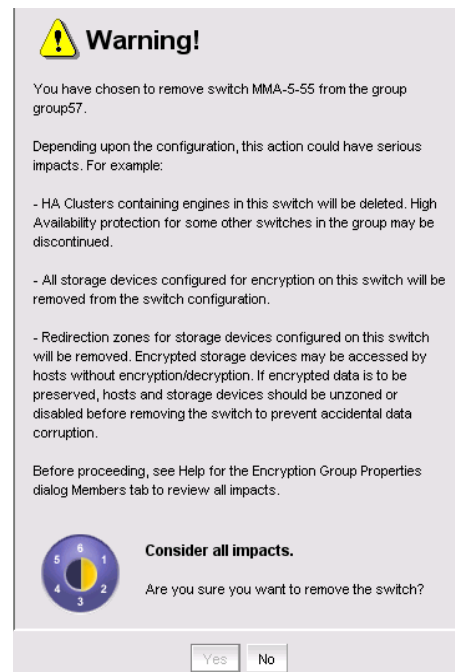
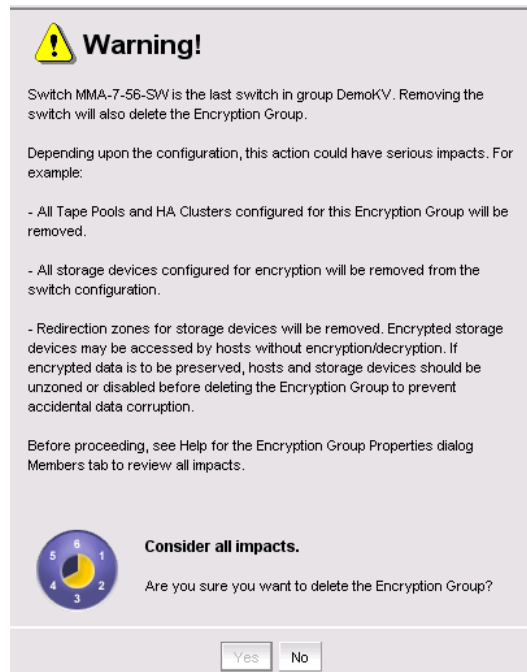
| Switch configuration                                                | Impact of removal                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The switch is the only switch in the encryption group.              | The encryption group is also removed.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| The switch has configured encryption targets on encryption engines. | <ul style="list-style-type: none"> <li>The switch is configured to encrypt traffic to one or more encryption targets.</li> <li>The target container configuration is removed.</li> <li>The encrypted data remains on the encryption target but is not usable until the encryption target is manually configured on another encryption switch.</li> </ul>                                                                                                            |
|                                                                     | <div style="text-align: right;">  <p><b>CAUTION</b></p> <p>The encryption target data is visible in encrypted format to zoned hosts. It is strongly recommended that you remove the encryption targets from all zones before you disable encryption. Otherwise, hosts may corrupt the encrypted data by writing directly to the encryption target without encryption.</p> </div> |
| The switch has encryption engines in HA Clusters.                   | The HA Clusters are removed. High availability is no longer provided to the other encryption engine in each HA Cluster.                                                                                                                                                                                                                                                                                                                                             |

Figure 259 shows the warning message that displays if you click **Remove** to remove a switch.



**FIGURE 259** Removal of switch warning

Figure 260 shows the warning message that displays if you click **Remove** to remove an encryption group.



**FIGURE 260** Removal of switch in encryption group warning

## Security tab

The **Security** tab (Figure 261) displays the status of the master key for the encryption group.

### NOTE

You must enable encryption engines before you back up or restore master keys.

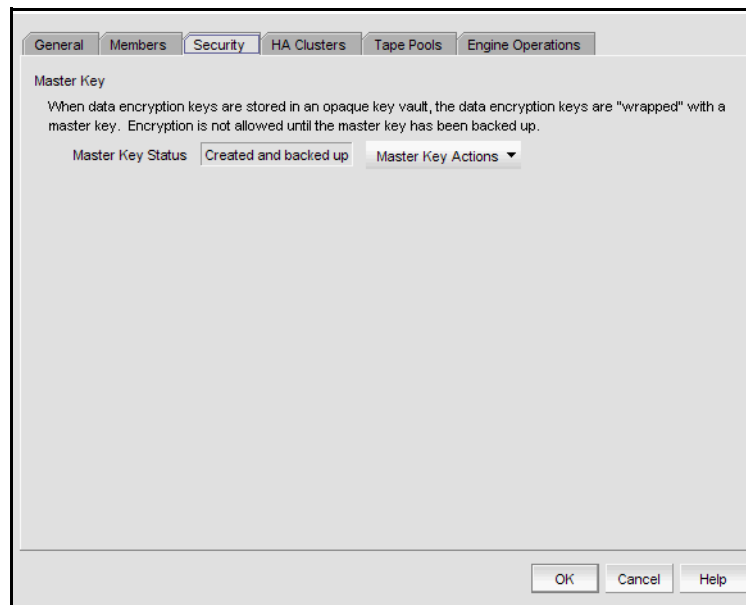
Master key actions are as follows:

- **Create a new master key**, which is enabled when no master key exists or the previous master key has been backed up.
- **Back up a master key**, which is enabled any time a master key exists.
- **Restore a master key**, which is enabled when either no master key exists or the previous master key has been backed up.

See “[Master keys](#)” on page 559 for complete information about managing master keys.

### NOTE

Encryption is not allowed until the master key has been backed up.



**FIGURE 261** Encryption Group Properties - Security tab

HA Clusters tab

HA clusters are groups of encryption engines that provide high availability features. If one of the engines in the group fails or becomes unreachable, the other cluster member takes over the encryption and decryption tasks of the failed encryption engine. An HA cluster consists of exactly two encryption engines. See “Creating high availability (HA) clusters” on page 541.

The **HA Clusters** tab (Figure 262) allows you to create and delete HA clusters, add encryption engines to and remove encryption engines from HA clusters, and failback an engine.

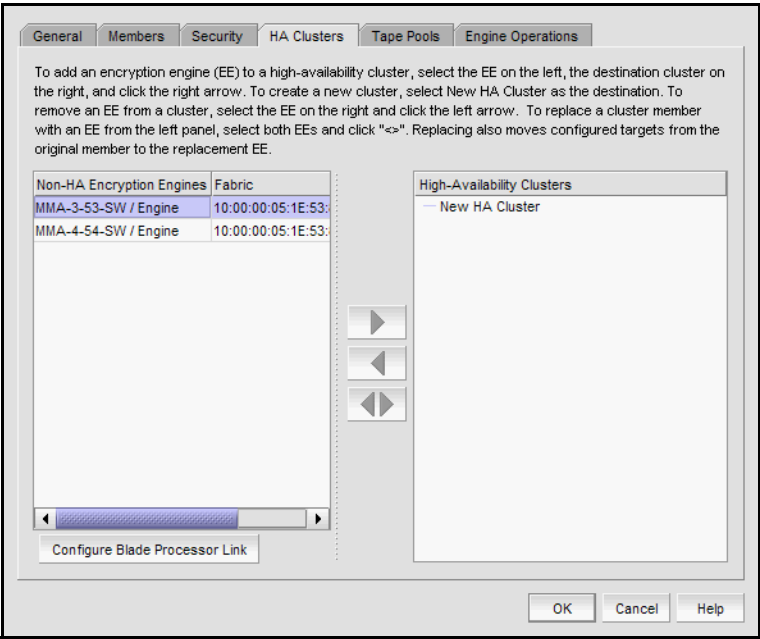


FIGURE 262 Encryption Group Properties - HA Clusters tab

Engine Operations tab

The **Engine Operations** tab enables you to replace an encryption engine in an encryption switch with another encryption engine in another switch within a DEK Cluster environment. A DEK Cluster is a set of encryption engines that encrypt the same target storage device. DEK Clusters do not display in the Management application, they are an internal implementation feature and have no user-configurable properties. Refer to “Replacing an encryption engine in an encryption group” on page 540.

NOTE

You cannot replace an encryption engine if it is part of an HA Cluster. For information about HA Clusters, refer to “HA Clusters tab” on page 584.

## Link Keys tab

Connections between a switch and an NetApp LKM key vault require a shared link key. Link keys are used only with LKM key vaults. They are used to protect data encryption keys in transit to and from the key vault. There is a separate link key for each key vault for each switch. The link keys are configured for a switch but are stored in the encryption engines, and all the encryption engines in a group share the same link keys. The **Link Keys** tab displays a table that shows link key status for each switch in an encryption group.

You must create link keys under the following circumstances:

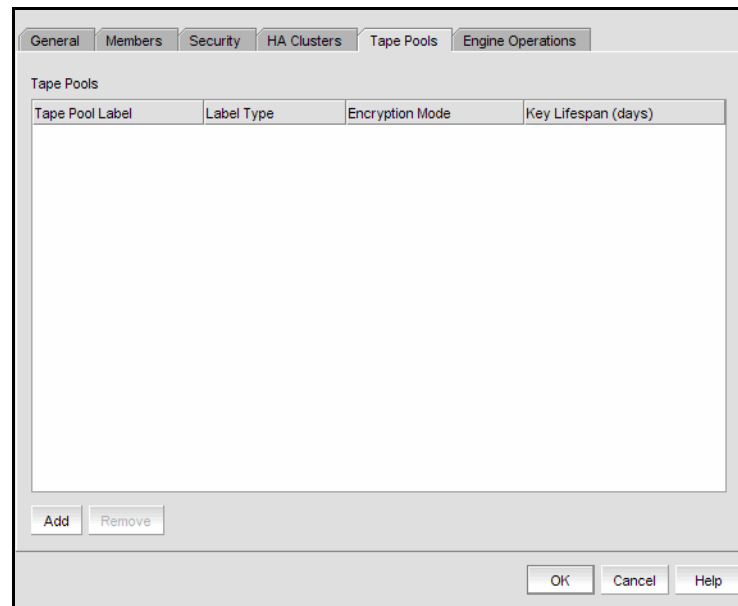
- When a new encryption group is created.
- When a new switch is added to an encryption group.
- When a new key vault is added to an encryption group.
- After all encryption engines in a switch have been zeroized.
- When all of the encryption blades have been removed from a director and one or more new encryption blades have been added.

Refer to [“Establishing the trusted link”](#) on page 508 for information on how the **Accept** and **Establish** buttons are used in establishing the trusted link between a switch and LKM.

## Tape Pools tab

Tape pools are managed from the **Tape Pools** tab.

[Figure 263](#) displays the tape pools tab.



**FIGURE 263** Encryption Group Properties - Tape Pools tab

- If you want to remove a tape pool, select one or more tape pools in the list and click **Remove**.
- To modify the tape pool, remove the entry and add a new tape pool. See [“Adding tape pools”](#) on page 586 for more information.

### *Tape pools overview*

Tape cartridges and volumes may be organized into a tape pool (a collection of tape media). The same data encryption keys are used for all cartridges and volumes in the pool. Tape pools are used by backup application programs to group all the tape volumes used in a single backup or in a backup plan. The tape pool name or number used must be the same name or number used by the host backup application. If the same tape pool name or number is configured for an encryption group, tapes in that tape pool are encrypted according to the tape pool settings instead of the tape LUN settings.

Encryption switches and encryption blades support tape encryption at the tape pool level (for most backup applications) and at the LUN (tape drive) level. Since Tape Pool policies override the LUN (tape drive) policies, the LUN pool policies are used only if no tape pools exist, or if the tape media/volume does not belong to any configured tape pools.

All encryption engines in the encryption group share the tape pool definitions. Tapes can be encrypted by an encryption engine, where the container for the tape target LUN is hosted. The tape media is mounted on the tape target LUN.

Tape pool definitions are not needed to read a tape. Tape pool definitions are only used when writing to tape.

### *Adding tape pools*

A tape pool can be identified by either a name or a number, but not both. Tape pool names and numbers must be unique within the encryption group. When a new encryption group is created, any existing tape pools in the switch are removed and must be added.

1. Select **Configure > Encryption** from the menu bar.

The **Encryption Center** dialog box displays.

2. If groups are not visible in the **Encryption Devices** table, select **View > Groups** from the menu bar.

The encryption groups display in the **Encryption Devices** table.

3. Select an encryption group from the tree, and select **Group > Tape Pools** from the menu bar, or right-click the encryption group and select **Tapepools**.

The **Add Tape Pool** dialog box displays. The **Name** tape pool label type is the default; however, you can change the tape pool label type to its number by selecting **Number**, shown in [Figure 265](#).

**FIGURE 264** Add Tape Pool by name dialog box

**FIGURE 265** Add Tape Pool by number dialog box

4. Specify the **Tape Pool Label Type**. Tape pools can be identified by either a name or a number, shown in [Figure 264](#) and [Figure 265](#).
5. Enter a name for the tape pool. If you selected **Number** as the **Tape Pool Label Type**, the name must match the tape pool label or tape ID/number that is configured on the tape backup/restore application.
6. Select the **Encryption Mode**.

Choices include **Clear Text**, **DF-Compatible Encryption**, and **Native Encryption**. **DF-Compatible Encryption** is valid only when LKM is the key vault. The **Key Lifespan (days)** field is editable only if the tape pool is encrypted. If **Clear Text** is selected as the encryption mode, the key lifespan is disabled.

**NOTE**

You cannot change the encryption mode after the tape pool I/O begins. DF-compatible encryption requires a DF-compatible encryption license to be present on the switch. If the license is not present, a warning message displays.

7. Enter the number of days that you want to use a key before obtaining a new key, if you want to enforce a key lifespan. The default is Infinite (a blank field or a value of 0).

**NOTE**

The key lifespan interval represents the key expiry timeout period for tapes or tape pools. You can only enter the **Key Lifespan** field if the tape pool is encrypted. If **Clear Text** is selected as the encryption mode, the **Key Lifespan** field is disabled.

8. Click **OK**.

## Encryption-related acronyms in log messages

Fabric OS log messages related to encryption components and features may have acronyms embedded that require interpretation. [Table 26](#) lists some of those acronyms.

**TABLE 26** Encryption acronyms

| Acronym | Name                      |
|---------|---------------------------|
| EE      | Encryption Engine         |
| EG      | Encryption Group          |
| HAC     | High Availability Cluster |



# Virtual Fabrics

---

## In this chapter

- [Virtual Fabrics overview](#) ..... 589
- [Virtual Fabrics requirements](#) ..... 590
- [Configuring Virtual Fabrics](#) ..... 592

## Virtual Fabrics overview

---


### NOTE

Virtual Fabrics requires that you have at least one Virtual Fabrics-enabled physical chassis running Fabric OS 6.2.0 or later in your SAN.

---

Virtual Fabrics enables you to divide one physical chassis into multiple logical switches that can be managed by separate administrators. Logical switches consist of one or more ports that act as a single FC switch. You can interconnect logical switches to create a logical fabric.

The following lists the benefits of using the Management application to manage Virtual Fabrics:

- Enables you to view your entire SAN (both physical and virtual) at a glance.
- Enables you to easily determine which devices in your SAN are logical switches. Logical switches are shown with a Virtual Fabrics icon (.
- Enables you to manage a logical switch the same as a physical switch, so that fewer physical chassis are required for Management application deployment.
- Enables you to use a logical switch for discovery and eliminate the requirement for one physical chassis for each fabric.
- Enables you to manage multiple Virtual Fabrics-capable physical chassis from the same interface.
- Enables you to provide logical isolation of data, control, and management paths at the port level.

Before using the Management application to manage Virtual Fabrics, you should familiarize yourself with Virtual Fabrics concepts, as described in the *Fabric OS Administrator's Guide*.

## Terminology

Table 27 lists definitions of Virtual Fabrics terms.

**TABLE 27** Virtual Fabrics terms

| Term                   | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physical chassis       | The physical switch or chassis from which you create logical switches and fabrics.                                                                                                                                                                                                                                                                                                                                                                 |
| Logical switch         | A collection of zero or more ports that act as a single Fibre Channel (FC) switch. When Virtual Fabrics is enabled on the chassis, there is always at least one logical switch: the default logical switch. You must assign each logical switch (default or general) in the same chassis to a different logical fabric. The logical switch supports all E_Ports and F_Ports. Note that EX_ports are only allowed on the base switch.               |
| Default logical switch | A logical switch that is created automatically when the Virtual Fabrics feature is enabled in a physical chassis. Initially, all ports in a chassis belong to the default logical switch. The default logical switch always exists as long as Virtual Fabrics is enabled. You cannot delete the default logical switch. The default logical switch supports all E_Ports and F_Ports.                                                               |
| Base switch            | A special logical switch used to communicate among different logical switches. The legacy EX_port is connected to the base logical switch. Inter-Switch Links (ISLs) connected to the base switch are used to communicate among different fabrics. The base switch supports E_Ports and EX_Ports.                                                                                                                                                  |
| Fabric ID (FID)        | An identifier you assign to a logical switch (default or general) or a base switch to designate to which logical or base fabric it belongs.                                                                                                                                                                                                                                                                                                        |
| Logical fabric         | A fabric with at least one logical switch.                                                                                                                                                                                                                                                                                                                                                                                                         |
| Base fabric            | A fabric formed from base switches that have the same FID. The base fabric provides the physical connectivity across multiple segments of a fabric over which logical switches in the fabric can establish logical connectivity.                                                                                                                                                                                                                   |
| Extended ISL (XISL)    | An ISL physically connected between two base switches that carries traffic for multiple logical fabrics. By default, logical switches are configured to be able to use XISLs; however, you can configure a logical switch to <i>not</i> use XISLs. XISL use is not supported in the following cases: <ul style="list-style-type: none"> <li>FICON logical fabrics</li> <li>Logical switches in an edge fabric connected to an FC router</li> </ul> |

## Virtual Fabrics requirements

To configure Virtual Fabrics, you must have at least one Virtual Fabrics-enabled physical chassis running Fabric OS 6.2.0 or later in your SAN. Use one of the following options to discover a Virtual Fabrics-enabled physical chassis on the Management application topology:

- Discover a Virtual Fabrics-capable seed physical chassis running Fabric OS 6.2.0 or later. Virtual Fabrics is disabled by default. This physical chassis displays as a legacy switch. Once discovered, you must enable Virtual Fabrics.
- Discover a Virtual Fabrics-enabled seed physical chassis running Fabric OS 6.2.0 or later with Virtual Fabrics enabled, and at least one logical switch defined on the core switch. The physical chassis displays as a virtual switch.
- Upgrade a physical chassis already in your SAN to Fabric OS 6.2.0 or later. Virtual Fabrics is disabled by default. This switch displays as a legacy switch. Once upgraded, you must enable Virtual Fabrics.

For more information about enabling Virtual Fabrics on a physical chassis, refer to [“Enabling Virtual Fabrics on a discovered device”](#) on page 593.

**Table 28** lists the Virtual Fabric-capable physical chassis and the number of logical switches allowed for each of those physical chassis.

**TABLE 28** Maximum number of logical switches per chassis

| Physical chassis          | Number of logical switches allowed |
|---------------------------|------------------------------------|
| 40-port, 8 Gbps FC Switch | 3                                  |
| 80-port, 8 Gbps FC Switch | 4                                  |
| 384-port Backbone Chassis | 8                                  |
| 192-port Backbone Chassis | 8                                  |

For the 40-port, 8 Gbps FC Switch and the 80-port, 8 Gbps FC Switch, any port can be assigned to any logical switch. However, depending on the partition type, the backbone chassis have the port requirements shown in [Table 29](#).

**TABLE 29** Blade and port types supported on logical switches

| Logical switch type    | Ports                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default logical switch | <ul style="list-style-type: none"> <li>• Extension Blade—E_, F_, GE_, and VE_Ports</li> <li>• FC 10-6 ISL Blade—E_ and F_Ports</li> <li>• FC 8 GB Port Blade—E_ and F_Ports</li> <li>• 10 Gig FCoE port Blade—E_ and F_Ports</li> <li>• 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension Blade <ul style="list-style-type: none"> <li>• FC ports: E_, F_, and VE_Ports</li> <li>• GE ports: VE_Ports</li> </ul> </li> <li>• 384-port and 192-port Backbone Chassis— ICL ports</li> </ul> |
| Logical switch         | <ul style="list-style-type: none"> <li>• Extension Blade—GE_ and VE_Ports</li> <li>• FC 8 GB Port Blade—E_ and F_Ports</li> <li>• 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension Blade <ul style="list-style-type: none"> <li>• FC ports: E_, F_, and VE_Ports</li> <li>• GE ports: VE_Ports</li> </ul> </li> <li>• 384-port and 192-port Backbone Chassis— ICL ports</li> </ul>                                                                                                       |
| Base switch            | <ul style="list-style-type: none"> <li>• Extension Blade—GE_ and VEX_Ports</li> <li>• FC 8 GB Port Blade—E_ and EX_Ports</li> <li>• 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension Blade <ul style="list-style-type: none"> <li>• FC ports: E_, EX_, VE_, and VEX_Ports</li> <li>• GE ports: VE_Ports</li> </ul> </li> <li>• 384-port and 192-port Backbone Chassis— ICL Ports</li> </ul>                                                                                              |

#### NOTE

In the 384-port Backbone Chassis, ports 48–63 of the FC 8 GB 64-port Blade are not supported in the base switch, and ports 56–63 are not supported as E\_Ports on the default logical switch. The 192-port Backbone Chassis does not have these limitations.

## Configuring Virtual Fabrics

The Management application allows you to discover, enable, create, and manage Virtual Fabric-capable physical chassis from the same interface.

This procedure describes the general steps you take to enable the Virtual Fabrics feature and configure logical fabrics. The logical fabrics in this example span multiple physical chassis, and the logical switches in each fabric communicate using an XISL in the base fabric.

1. Enable Virtual Fabrics in each physical chassis.  
See [“Enabling Virtual Fabrics on a discovered device”](#) on page 593 for instructions.
2. Set up base switches in each physical chassis:
  - a. Create base switches in each physical chassis and assign ports to them.  
See [“Creating a logical switch or base switch”](#) on page 593 for instructions.
  - b. Disable the base switches in each physical chassis.  
Right-click each base switch in the Connectivity Map or Product List and select **Enable/Disable > Disable**.
  - c. Physically connect ports in the base switches to form XISLs.
  - d. Enable all of the base switches. This forms the base fabric.  
Right-click each base switch in the Connectivity Map or Product List and select **Enable/Disable > Enable**.
3. Set up logical switches in each physical chassis:
  - a. Create logical switches in each physical chassis and assign ports to them. Make sure the logical switches are configured to allow XISL use (this is the default).  
See [“Creating a logical switch or base switch”](#) on page 593 for instructions.
  - b. Disable all of the logical switches in each physical chassis.  
Right-click each logical switch in the Connectivity Map or Product List and select **Enable/Disable > Disable**.
  - c. Physically connect devices and ISLs to the ports on the logical switches.  
You can connect ISLs from one logical switch to another logical switch in a different physical chassis only if the two logical switches have the same FID (and are thus in the same logical fabric). Traffic between these logical switches can travel over either this ISL or the XISL in the base fabric. The physical ISL path is favored over the XISL path because it has a lower cost.
  - d. Enable all logical switches in each chassis.  
Right-click each logical switch in the Connectivity Map or Product List and select **Enable/Disable > Enable**.

The logical fabric is formed.

## Enabling Virtual Fabrics on a discovered device

---

**ATTENTION**

Enabling Virtual Fabrics is disruptive. You should disable the physical chassis before you enable Virtual Fabrics.

---

---

**ATTENTION**

If the physical chassis is participating in a fabric, the affected fabric will be disrupted.

---

1. Right-click the physical chassis in the topology and select **Enable Virtual Fabric**.  
For a list of physical chassis that are Virtual Fabrics-capable, refer to [“Virtual Fabrics requirements”](#) on page 590.
2. Click **OK** on the warning message.  
Note that all ports are placed in the default logical switch and any EX\_ports are persistently disabled.

## Disabling Virtual Fabrics on a discovered device

To disable Virtual Fabrics, right-click the physical chassis in the Chassis group in the Product List and select **Disable Virtual Fabric**.

---

**ATTENTION**

Disabling Virtual Fabrics causes the physical chassis to reboot.

---

---

**ATTENTION**

Disabling Virtual Fabrics deletes all logical switches and returns port management to the physical chassis. If these logical switches are participating in a fabric, all affected fabrics will be disrupted.

---

## Creating a logical switch or base switch

---

**NOTE**

Virtual Fabrics must be enabled on at least one physical chassis in your fabric.

---

Optionally, you can define the logical switch to be a base switch. Each chassis can have only one base switch.

1. Select a switch with Virtual Fabrics enabled on the Product List or Connectivity Map and select **Configure > Logical Switches**.  
The **Logical Switches** dialog box displays.
2. Select the physical chassis from which you want to create a logical switch in the **Chassis** list.

3. Select one of the following in the **Existing Logical Switches** table:

- A physical chassis in the Discovered Logical Switches node.
- A NewFabric logical switch template in the Discovered Logical Switches node.
- The Undiscovered Logical Switches node.

If you select a logical switch template, the fabric-wide settings for the logical switch are obtained from the settings in the template.

If you select a physical chassis or the Undiscovered Logical Switches node, the fabric-wide settings for the logical switch are the default settings.

4. Click **New Switch**.

The **New Logical Switch** dialog box displays.

5. Click the **Fabric** tab, if necessary.

6. Enter a fabric identifier in the **Logical Fabric ID** field.

This assigns the new logical switch to a logical fabric.

If the logical fabric does not exist, this creates a new logical fabric as well as assigning the new logical switch.

7. (Optional) Clear the **Base Fabric for Transport** check box to configure the switch to *not* use XISLs.

By default, the logical switch is configured to use XISLs; however, you should clear the **Base Fabric for Transport** check box, because XISL use is not supported in the following cases:

- FICON logical fabrics
- Logical switches in an edge fabric connected to an FC router
- Logical switch in InteropMode 2 or InteropMode 3
- VE\_Ports of the 8 Gbps 12-FC port, 10 GbE ports, 2 - 10 GbE ports Extension Blade are to be added to the logical switch

8. (Optional) Perform the following steps to make the logical switch a base switch:

- a. Clear the **Base Fabric for Transport** check box.

This check box is not relevant for base switches because all base switches can use XISLs.

- b. Select the **Base Switch** check box.

9. (Optional) For Backbone Chassis only, select an option in the **256 Area Limit** list to use 256-area addressing mode (zero-based or port-based) or to disable this mode (default).

The 256-area addressing mode can be used in FICON environments, which have strict requirements for 8-bit area FC addresses.

10. (Optional) Enter new values for the fabric-wide parameters or leave unchanged to accept the current values.

Click the **Help** button for detailed information on each parameter.

11. Click the **Switch** tab.

12. Enter a name for the logical switch in the **Name** field.

13. Select a domain ID in the **Preferred Domain ID** list.

In a FICON environment, select a domain ID that is not in use by the default or another logical switch in the same chassis.

14. (Optional) Select the **Insistent** check box to not allow the domain ID to be changed when a duplicate domain ID exists.

If you select this check box and a duplicate domain ID exists, the switch will segment from the fabric instead of changing the domain ID.

15. Click **OK** on the **New Logical Switch** dialog box.

The new logical switch displays in the **Existing Logical Switches** table (already highlighted). This logical switch has no ports.

16. Select the ports you want to include in the logical switch from the **Ports** table.

17. Click the right arrow button.

The ports display in the selected logical switch node in the **Existing Logical Switches** table.

18. Click **OK** on the **Logical Switches** dialog box.

The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

---

#### NOTE

Ports are disabled before moving from one logical switch to another.

---

19. Select the **Re-Enable ports after moving them** check box.

20. (Optional) Select the **Unbind Port Addresses while moving them** check box.

21. Click **Start** to send these changes to the affected chassis.

---

#### NOTE

Most changes to logical switches will disrupt data traffic in the fabric.

---

The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

22. When the changes are complete, click **Close**.

23. If the newly created switch is not part of a discovered fabric, then you must discover the switch.

- a. Undiscover the physical chassis. See [“Deleting a fabric”](#) on page 41 for instructions.
- b. Rediscover the physical chassis. See [“Discovering fabrics”](#) on page 36 for instructions.

When entering the IP address, use the IP address of the physical fabric.

## Finding the physical chassis for a logical switch

The Management application enables you to locate the physical chassis in the Product List from which the logical switch was created.

To find the physical chassis for a logical switch, right-click the logical switch in the Connectivity Map or Product List and select **Chassis**.

The physical chassis is highlighted in the Product List.

## Finding the logical switch from a physical chassis

The Management application enables you to locate the logical switch from the physical chassis.

To find the logical switch, right-click the physical chassis within the **Chassis Group** in the Product List and select **Logical Switches > Logical\_Switch\_Name**.

The logical switch you selected is highlighted in the Product List and Connectivity Map.

## Assigning ports to a logical switch

A port can be assigned to only one logical switch.

All ports are initially assigned to the default logical switch. When you create a logical switch, it has no ports and you must explicitly assign ports to it.

When you assign a port to a logical switch, it is removed from the original logical switch and assigned to the new logical switch.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Logical Switches**.

The **Logical Switches** dialog box displays.

2. Select the physical chassis from which you want to assign ports in the **Chassis** list.
3. Select the ports you want to include in the logical switch from the **Ports** table.
4. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.
5. Select the logical switch in the **Existing Logical Switches** table.
6. Click the right arrow button.

The ports display in the selected logical switch node in the **Existing Logical Switches** table.

7. Click **OK** on the **Logical Switches** dialog box.

The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

---

### NOTE

Ports are disabled before moving from one logical switch to another.

---

8. Select the **Re-Enable ports after moving them** check box.
9. (Optional) Select the **Unbind Port Addresses while moving them** check box.
10. Click **Start** to send these changes to the affected chassis.

---

### NOTE

Most changes to logical switches will disrupt data traffic in the fabric.

---

The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

11. When the changes are complete, click **Close**.

## Removing ports from a logical switch

1. Select a switch on the Product List or Connectivity Map and select **Configure > Logical Switches**.

The **Logical Switches** dialog box displays.

2. Select the physical chassis to which the ports belong in the **Chassis** list.
3. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.
4. Select the ports you want to remove from the logical switches from the **Existing Logical Switches** table.
5. Click the left arrow button.

A message displays indicating that the ports will be moved to the default logical switch.

6. Click **OK** on the **DCFM Warning** message.

The selected ports are removed from the logical switch and automatically reassigned to the default logical switch. The selected ports are highlighted in the **Ports** table.

7. (Optional) Perform the following steps to assign the ports to a logical switch other than the default logical switch:
  - a. Select the destination logical switch in the **Existing Logical Switches** table.
  - b. Click the right arrow button.

The ports display in the selected logical switch node in the **Existing Logical Switches** table.

8. Click **OK** on the **Logical Switches** dialog box.

The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

---

### NOTE

Ports are disabled before moving from one logical switch to another.

---

9. Select the **Re-Enable ports after moving them** check box.
10. (Optional) Select the **Unbind Port Addresses while moving them** check box.
11. Click **Start** to send these changes to the affected chassis.

---

### NOTE

Most changes to logical switches will disrupt data traffic in the fabric.

---

The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

12. When the changes are complete, click **Close**.

## Deleting a logical switch

1. Select a switch on the Product List or Connectivity Map and select **Configure > Logical Switches**.

The **Logical Switches** dialog box displays.

2. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.
3. Select the logical switch you want to delete from the **Existing Logical Switches** table and click **Delete**.

All ports in the deleted logical switch are reassigned to the default logical switch.

4. Read the confirmation message and click **Yes**.
5. Click **OK** on the **Logical Switches** dialog box.

The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

---

### NOTE

Ports are disabled before moving from one logical switch to another.

---

6. Select the **Re-Enable ports after moving them** check box.
7. (Optional) Select the **Unbind Port Addresses while moving them** check box.
8. Click **Start** to send these changes to the affected chassis.

---

### NOTE

Most changes to logical switches will disrupt data traffic in the fabric.

---

The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

9. When the changes are complete, click **Close**.

## Configuring fabric-wide parameters for a logical fabric

When you create a logical switch, you must assign it to a fabric and configure fabric-wide parameters. All the switches in a fabric must have the same fabric-wide settings.

Instead of configuring these settings separately on each logical switch, you can create a *logical fabric template*, which defines the fabric-wide settings for a logical fabric. Then, when you create logical switches for that fabric, these fabric-wide settings are used automatically and you do not have to re-enter them.

Creating a logical fabric template does *not* create a logical fabric. A logical fabric is created only when you assign logical switches to a fabric ID (FID).

The logical fabric template exists only in the lifetime and scope of the **Logical Switches** dialog box. When you exit this dialog box, the logical fabric templates are deleted.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Logical Switches**.

The **Logical Switches** dialog box displays.

2. Select the physical chassis from which you want to create a logical fabric in the **Chassis** list.

3. Click **New Fabric**.

The **New Logical Fabric Template** dialog box displays.

4. Enter a new identifier in the **Logical Fabric ID** field to create a new logical fabric template.

This identifier is how you distinguish among multiple logical fabric templates in the **Logical Switches** dialog box. If you create more than one logical fabric template, give them different fabric IDs.

5. Enter new values for the fabric parameters or leave unchanged to accept the default values.

Click the **Help** button for detailed information on each parameter.

---

#### NOTE

If you set the long distance fabric, it must be set on all devices in the fabric.

---

6. Click the **Switch** tab.

7. Select the **Insistent Domain ID** check box to guarantee that a switch operates only with its preassigned domain ID. If a duplicate domain ID exists, the switch will segment from the fabric instead of changing the domain ID.

Leave this check box blank to allow the domain ID to be changed if a duplicate address exists.

8. Click **OK** on the **New Logical Fabric Template** dialog box.

The new logical fabric template displays under the **Discovered Logical Switches** node in the **Existing Logical Switches** table (already highlighted).

All of the logical fabric templates have the same name, "NewFabric". You can differentiate among the templates by the FID number.

You can now create logical switches using the fabric-wide settings in the logical fabric template. To assign logical switches, refer to ["Creating a logical switch or base switch"](#) on page 593.

---

#### NOTE

When you close the **Logical Switches** dialog box, the logical fabric templates are automatically deleted. Create the logical switches first, before closing the dialog box, to use the template.

---

## Applying logical fabric settings to all associated logical switches

You can apply a selected logical switch configuration to all logical switches in the same fabric. This configures the fabric parameters for the selected logical switch to all logical switches in the fabric.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Logical Switches**.

The **Logical Switches** dialog box displays.

2. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.

3. Right-click the logical switch for which you have configured logical fabric settings from the **Existing Logical Switches** table and select **Configure All**.

The logical fabric configuration settings (**Fabric** tab) are applied to all logical switches in the same fabric (determined by FID).

4. Click **OK** on the **Logical Switches** dialog box.

The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

---

**NOTE**

Ports are disabled before moving from one logical switch to another.

---

5. Select the **Re-Enable ports after moving them** check box.
6. (Optional) Select the **Unbind Port Addresses while moving them** check box.
7. Click **Start** to send these changes to the affected chassis.

---

**NOTE**

Most changes to logical switches will disrupt data traffic in the fabric.

---

The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

8. When the changes are complete, click **Close**.

## Moving a logical switch to a different fabric

You can move a logical switch from one fabric to another by assigning a different fabric ID.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Logical Switches**.

The **Logical Switches** dialog box displays.

2. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.
3. Select the logical switch you want to move to another logical fabric.
4. Click **Edit**.

The **Edit Properties** dialog box displays.

5. Change the FID in the **Logical Fabric ID** field.
6. Click **OK** on the **Edit Properties** dialog box.

The logical switch displays under the new logical fabric node in the **Existing Logical Switches** table.

7. Click **OK** on the **Logical Switches** dialog box.

The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

---

**NOTE**

Ports are disabled before moving from one logical switch to another.

---

8. Select the **Re-Enable ports after moving them** check box.
9. (Optional) Select the **Unbind Port Addresses while moving them** check box.

10. Click **Start** to send these changes to the affected chassis.

---

**NOTE**

Most changes to logical switches will disrupt data traffic in the fabric.

---

The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

11. When the changes are complete, click **Close**.
12. If the newly created switch is not part of a discovered fabric, then you must discover the switch.
  - a. Undiscover the physical chassis. See [“Deleting a fabric”](#) on page 41 for instructions.
  - b. Rediscover the physical chassis. See [“Discovering fabrics”](#) on page 36 for instructions.

When entering the IP address, use the IP address of the physical fabric.

## Changing a logical switch to a base switch

The **Base Switch** column in the **Existing Logical Switches** table indicates whether a logical switch is a base switch.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Logical Switches**.

The **Logical Switches** dialog box displays.

2. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.
3. Select the logical switch you want to change to a base switch.
4. Click **Edit**.

The **Edit Properties** dialog box displays.

5. Clear the **Base Fabric for Transport** check box.

This check box is applicable only to logical switches that are *not* base switches.

6. Select the **Base Switch** check box.
7. Click **OK** on the **Edit Properties** dialog box.

The **Base Switch** column in the **Existing Logical Switches** table now displays **Yes** for the logical switch.

8. Click **OK** on the **Logical Switches** dialog box.

The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

---

**NOTE**

Ports are disabled before moving from one logical switch to another.

---

9. Select the **Re-Enable ports after moving them** check box.
10. (Optional) Select the **Unbind Port Addresses while moving them** check box.

## 21 Changing a logical switch to a base switch

11. Click **Start** to send these changes to the affected chassis.

---

**NOTE**

Most changes to logical switches will disrupt data traffic in the fabric.

---

The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

12. When the changes are complete, click **Close**.

# Zoning

---

## In this chapter

- [Zoning overview](#) . . . . . 603
- [Zoning configuration](#) . . . . . 607
- [LSAN zoning](#) . . . . . 628
- [Traffic isolation zoning](#) . . . . . 632
- [Zoning administration](#) . . . . . 638

## Zoning overview

Zoning defines the communication paths in a fabric. A zone is a collection of initiator and target ports within the SAN. The ports in a zone can only communicate with other ports in that zone. However, ports can be members of more than one zone.

Zoning is a fabric management service that can be used to create logical subsets of devices within a SAN and enable partitioning of resources for management and access control purposes. Zoning allows only members of a zone to communicate within that zone. All others attempting to access from outside the zone are rejected, hence zoning also provides a security function.

Zoning provides software zoning controlled at the Node World Wide Name (nWWN) level assisted by the name server of a switch. Depending on the vendor and interoperability mode, it also supports Domain/Port zoning. Domain/Port zoning is not supported when the fabric is in McDATA Open Mode (InteropMode 3).

### Types of zones

Fabric OS has the following types of zones:

- **Regular zones**  
Enable you to partition your fabric into logical groups of devices that can access each other. These are “regular” or “normal” zones. Unless otherwise specified, all references to zones in this chapter refer to these regular zones.
- **Frame redirection zones**  
Re-route frames between an initiator and target through a Virtual Initiator and Virtual Target for special processing or functionality, such as for storage virtualization or encryption. See [“Redirection zones”](#) on page 572 for more information.
- **LSAN zones**  
Provide device connectivity between fabrics without merging the fabrics. See [“LSAN zoning”](#) on page 628 for more information.

- **QoS zones**  
Assign high or low priority to designated traffic flows. Quality of Service (QoS) zones are normal zones with additional QoS attributes that you select when you create the zone.
- **Traffic Isolation zones (TI zones)**  
Isolate inter-switch traffic to a specific, dedicated path through the fabric. See [“Traffic isolation zoning”](#) on page 632 for more information.

## Online zoning

Online zoning allows you to do the following:

- View both defined and active zone information in the fabric.
- Create and modify zones and zone configurations in the software zone database.
- Activate a zone configuration in order to publish the zone information in the selected fabric.
- Deactivate the current active zone configuration.
- Configure zoning policies in the selected fabric.
- Generate zoning reports for the fabric.

---

### NOTE

Online zoning is supported only in Brocade Native mode (InteropMode 0) and in a mixed Fabric OS and M-EOS McDATA Fabric Mode (InteropMode 2).

For pure EOS fabrics in McDATA Fabric Mode (InteropMode 2) or McDATA Open Mode (InteropMode 3) and for mixed Fabric OS and M-EOS fabrics in McDATA Open Mode, only offline zoning is available.

---

## Offline zoning

Offline zoning enables you to copy a fabric zone DB and edit it offline. The benefits to offline zoning include the following:

- You want to make changes to the zone database now, but apply them later.  
For example:
  - If you make incremental changes to zoning on an ongoing basis, but want to apply the changes to the fabric during scheduled downtime.
  - If you are expecting new servers to be delivered, but want to make changes to zoning now and apply the changes after the servers are delivered and ready to go online.
- You want to keep multiple copies of the zone database and switch between them.  
For example, if you want to allow specific servers access to tape drives for backup during specific time windows, you can have multiple zone databases (one or more for backup and one for normal operation) and switch between them easily.
- You want to analyze the impact of changes to storage access before applying the changes.  
For example, if you deploy a new server and want to ensure that the zoning changes result in only the new server gaining access to specific storage devices and nothing else. See [“Comparing zone databases”](#) on page 638.

## Accessing zoning

Most of the zoning tasks are performed from the Zoning dialog box. You can access the Zoning dialog box from the main screen of the Management application using any of the following methods:

- Select **Configure > Zoning > Fabric**.
- Click the **Zoning** icon on the toolbar.
- Right-click a port, switch, switch group, or fabric in the device list and select **Zoning**.
- Right-click a port, switch, switch group, or fabric in the Connectivity Map and select **Zoning**.

## Zoning naming conventions

The naming rules for zone names, zone aliases, and zone configuration names vary with the type of fabric.

The following conventions apply to Fibre Channel fabrics:

- Names are case sensitive in McDATA Open Mode. However, names are *not* case sensitive in Brocade Native Mode or McDATA Fabric Mode.
- Zone, alias, and configuration names cannot begin with “red\_”, “lsan\_red\_”, or “d\_\_efault\_\_”. Zone configuration names cannot begin with “r\_e\_d\_i\_r\_c\_\_fg”. These prefixes are reserved.
- Names cannot begin with a numeric character or a special character.
- Recommended character limit: 64 characters.
- Duplicate names are not allowed between zones, zone aliases, and zone configurations within a zone database.

If you enter an invalid zone or zone configuration name, an error or warning message displays depending on the type of fabric you are trying to zone:

For FC fabrics, if an invalid name is entered for a zone or zone configuration, the application displays a warning message. If there is a naming violation according to the vendor, the switch returns the error message for the exact information along with the zone configuration activation failure message.

## Administrator zoning privileges

You can set read-only or read/write access for the following zoning components:

- LSAN Zoning
- Zoning Activation (and deactivation)
- Zoning Offline
- Zoning Online
- Zoning Set Edit Limits

When read/write privileges are defined for all components, an administrator can perform all zoning-related operations provided by dialog boxes and shortcut menus. [Table 30](#) summarizes the functions permitted for other privilege level settings.

TABLE 30 Privilege levels and accessible zoning functions

| Privilege level per zoning components                                                                                                                     | Accessible functions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Read-only <ul style="list-style-type: none"> <li>• Activation</li> <li>• LSAN</li> <li>• Offline</li> <li>• Online</li> <li>• Set Edit Limits</li> </ul>  | <b>Zone DB</b> tab <ul style="list-style-type: none"> <li>• Zoning Policies</li> <li>• Find</li> </ul> <b>Active Zone Config</b> tab <ul style="list-style-type: none"> <li>• No accessible functions</li> </ul> <b>Potential Members</b> list shortcut menu <ul style="list-style-type: none"> <li>• Product Label</li> <li>• Port Label</li> <li>• Port Display</li> <li>• List Zone Members</li> <li>• Show Connected End Devices</li> <li>• Display All</li> <li>• Table</li> </ul> <b>Zones</b> list shortcut menu <ul style="list-style-type: none"> <li>• Port Label</li> <li>• Properties</li> <li>• Tree</li> </ul> <b>Zone Config</b> list shortcut menu <ul style="list-style-type: none"> <li>• Properties</li> <li>• Tree</li> </ul> <b>Set Change Limits for Zoning Activation</b> dialog box <ul style="list-style-type: none"> <li>• No accessible functions</li> </ul> |
| Read/write <ul style="list-style-type: none"> <li>• Activation</li> <li>• LSAN</li> <li>• Offline</li> <li>• Online</li> <li>• Set Edit Limits</li> </ul> | All functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Note the following items about setting zoning privileges:

- If no privilege level is set for any of the components, zoning is disabled at the Management application main menu and the **Zoning** dialog box cannot be opened.
- If a privilege level is set for Activation without levels being set for the Offline, Online, or LSAN Zoning, the **Zoning** dialog box cannot be opened. The Activation privilege cannot be added without setting at least one privilege above to either Read/Write or Read-Only. An information message displays when attempting to add the Zoning Activation only privilege.
- If a privilege level is set for the Offline, Online, or LSAN Zoning, or for all three, without a level being set for Activation, the **Zoning** dialog box can be opened and the functions outlined in the table for read/write and read-only settings for the libraries will be accessible. (Activating and deactivating active zone configurations will not be possible.)

## Zoning configuration

At a minimum, zoning configuration entails creating zones and zone members. However, you can also create zone aliases, zone configurations, and zone databases. You can define multiple zone configurations, deactivating and activating individual configurations as your needs change. Zoning configuration can also involve enabling or disabling safe zoning mode and the default zone.

The supported maximum zone database size is 1 MB.

### Configuring zoning for the SAN

The following procedure provides an overview of the steps you must perform to configure zoning for the SAN.

Note that for any zoning-related procedure, changes to a zone database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box. If you click **Cancel** or the close button (X), no changes are saved.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all the discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.

5. Create the zones.

For specific instructions, refer to [“Creating a new zone”](#) on page 608.

6. Add members to each zone.

For specific instructions, refer to [“Adding members to a zone”](#) on page 609 and [“Creating a new member in an LSAN zone”](#) on page 630.

7. Create a zone configuration.

For specific instructions, refer to [“Creating a zone configuration”](#) on page 618.

8. Activate the zone configuration.

For specific instructions, refer to [“Activating a zone configuration”](#) on page 620.

9. Set zoning policies for FC fabrics, if necessary.

For specific instructions, refer to [“Enabling or disabling the default zone for fabrics”](#) on page 614 and [“Enabling or disabling safe zoning mode for fabrics”](#) on page 615.

10. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Creating a new zone

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **New Zone**.

A new zone displays in the **Zones** list.

5. Type the desired name for the zone.

For zone name requirements and limitations, refer to [“Zoning naming conventions”](#) on page 605.

6. (Optional—Fabric OS only) Set the QoS for the zone by right-clicking the zone and selecting **QoS > Priority\_Level** (High, Medium, or Low).

---

### NOTE

QoS priority support is available for zones with WWN or Domain,Index (D,I) members.

QoS zones using D,I notation cannot be created if any of the switches in the fabric are running Fabric OS versions earlier than 6.3.0.

---

The zone name is automatically renamed to QoSX\_Zone\_Name, where X is the priority level (H—High, M—Medium, or L—Low) and Zone\_Name is the name you entered for the zone.

7. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:
  - a. Select **Save to Switch** from the **Zone DB Operation** list.
  - b. Click **Yes** on the confirmation message.

The selected zone database is saved to the fabric without enabling a specific zone configuration.

8. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

If the zone is empty, a warning message displays.

## Viewing zone properties

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the zone you want to review in the **Zones** list and select **Properties**.

The **Zone Properties** dialog box displays.

5. Review the zone properties.

Depending on what type of zone you selected, the following information is included in the zone properties:

- **Zone Name**—The name of the zone.
- **Zone Configs Containing This Zone**—The number of zone configurations to which this zone belongs.
- **Total Zone Members**—The number of zone members in the selected zone.
- **Number of Aliases**—The number of aliases in this zone.
- **Zone Members Contained by Aliases**—The number of zone members in the selected alias.
- **Configure Status** (TI Zone and Fabric OS only)—Whether or not the TI zone is enabled.
- **Configure Failover** (TI Zone and Fabric OS only)—Whether or not the TI zone failover is enabled.
- **Status** (not applicable for TI zones)—The status of the selected zone.

6. Click **OK** to close the **Zone Properties** dialog box.

## Adding members to a zone

Use this procedure to add a member to a zone when the member is listed in the **Potential Members** list of the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

If you want to show all the discovered fabrics in your fabric group in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.

4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

5. Select an option from the **Type** list.

By default, the first time you launch the **Zoning** dialog box for a Zoning Scope, the **Potential Members** list displays valid members using the following rules:

- If you select the **World Wide Name** type, the valid members display by the Attached Ports.
- If you select the **Domain/Port Index** type, the valid members display by the ALL Product Ports (both occupied and unoccupied). This option is available for FC fabrics only.
- If you select the **Alias** type, the valid members display by the device Alias.

6. Select one or more members to add to the zone in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member. To add all ports on a device, select the device.)
7. Click the right arrow between the **Potential Members** list and **Zones** list to add the selected members to the zone.

A message may display informing you that one or some of the selected potential members cannot be zoned. Click **OK** to close the message box. Reconsider your selections and make corrections as appropriate.

8. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:
  - a. Select **Save to Switch** from the **Zone DB Operation** list.
  - b. Click **Yes** on the confirmation message.

The selected zone database is saved to the fabric without enabling a specific zone configuration.

9. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Creating a new member in a zone by WWN

Use this procedure to add a member to a zone when the member is not listed in the **Potential Members** list of the **Zone DB** tab.

For instructions to add a member to a zone when the member is listed in the **Potential Members** list, refer to the procedure [“Adding members to a zone”](#) on page 609.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

5. Click **New Member**.

The **Add Zone Member** dialog box displays.

6. Select **World Wide Name** from the **Member Type** list.
7. Add the new member by port name by completing the following steps.
  - a. Select the **Existing End Device Node/Port Name** option.
  - b. Select a port name from the list.

OR

Add the new member by port WWN by completing the following steps.

- a. Select the **End Device Node/Port WWN** option.
- b. Enter a port WWN in the **End Device Node/Port WWN** field.

If you enter a WWN that has been used by a discovered device, a message displays informing you of this and instructing you to enter a port WWN. Click **OK** to close the message box and enter an appropriate WWN.

- c. (Optional) Click the **Assign Name** check box and enter a name in the field.

If a name was previously assigned, the name appears in the field and a message displays asking whether you want to overwrite the existing name. Click **Yes** to continue and assign a new name, or **No** to decline and close the message box.

8. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

OR

Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat steps 5, 6, and 7 as many times as needed, and proceed to step 8 when appropriate.

9. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:
  - a. Select **Save to Switch** from the **Zone DB Operation** list.
  - b. Click **Yes** on the confirmation message.

The selected zone database is saved to the fabric without enabling a specific zone configuration.

10. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Creating a new member in a zone by domain, port index

Use this procedure to add a member to a zone when the member is not listed in the **Potential Members** list of the **Zone DB** tab.

For instructions to add a member to a zone when the member is listed in the **Potential Members** list, refer to the procedure [“Adding members to a zone”](#) on page 609.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

5. Click **New Member**.

The **Add Zone Member** dialog box displays.

6. Select **Domain, Port Index** from the **Member Type** list.

7. Add the new member by port name by completing the following steps.

- a. Select the **Existing Switch Port Name** option.
- b. Select a name from the list.

OR

Create a new member by domain and port index by choosing one of the following options:

- Select the **Domain, Port Index (decimal)** option and enter domain and port values in the fields.
- Select the **Domain, Port Index (hex)** option and enter domain and port values in the fields.

8. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

OR

Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat steps 5, 6, and 7 as many times as needed, and proceed to step 8 when appropriate.

9. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:

- a. Select **Save to Switch** from the **Zone DB Operation** list.
- b. Click **Yes** on the confirmation message.

The selected zone database is saved to the fabric without enabling a specific zone configuration.

10. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Creating a new member in a zone by alias

Use this procedure to add a member to a zone when the member is not listed in the **Potential Members** list of the **Zone DB** tab. For instructions to add a member to a zone when the member is listed in the **Potential Members** list, refer to the procedure [“Adding members to a zone”](#) on page 609.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

5. Click **New Member**.

The **Add Zone Member** dialog box displays.

6. Select **Alias** from the **Member Type** list.

7. Add the new member by alias name by completing the following steps.

- a. Select the **Existing Alias** option.
- b. Select an alias from the list.

OR

Create a new alias by completing the following steps.

- a. Select the **New Alias** option.
- b. Enter a name in the **New Alias** field.
- c. Assign the alias by choosing one of the following options:
  - Select the **WWN** option and enter the WWN in the field.  
If you enter a WWN that has been used by a discovered device, a message displays informing you of this and instructing you to enter a port WWN. Click **OK** to close the message box and enter an appropriate WWN.
  - Select the **Domain, Port Index (decimal)** option and enter domain or port values in the fields.
  - Select the **Domain, Port Index (hex)** option and enter domain or port values in the fields.

8. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

OR

Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat steps 5, 6, and 7 as many times as needed, and proceed to step 8 when appropriate.

9. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:
  - a. Select **Save to Switch** from the **Zone DB Operation** list.
  - b. Click **Yes** on the confirmation message.
 

The selected zone database is saved to the fabric without enabling a specific zone configuration.
10. Click **OK** or **Apply** to save your changes.
 

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Enabling or disabling the default zone for fabrics

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zoning database you want from the **Zone DB** list.
5. Click **Zoning Policies**.

The **Zoning Policies** dialog box displays.

---

### NOTE

The format and content of this dialog box vary slightly depending on Interop Mode, the target selected in the **Zoning Scope** list, and whether safe zoning mode is enabled. If safe zoning mode is enabled, the **Default Zone** button is disabled. If you want to enable the default zone, you must disable the safe zoning mode.

---

6. Make sure the appropriate fabric is named on the **Zoning Policies** dialog box.
7. Perform one of the following actions based on the task you want to complete:
  - To enable the default zone, click **Enable**, and then click **OK**.
  - To disable the default zone, click **Disable**, and then click **OK**.

The **Zoning Policies** dialog box closes and the **Zone DB** tab displays.

8. Click **OK** or **Apply** to save your changes.
 

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Enabling or disabling safe zoning mode for fabrics

---

### NOTE

Safe Zoning Mode is available only on devices running in McDATA Fabric Mode and, for pure EOS fabrics, in McDATA Open Mode.

---

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **Zoning Policies**.

The **Zoning Policies** dialog box displays.

---

### NOTE

The format and content of this dialog box vary slightly depending on Interop Mode and the target selected in the **Zoning Scope** list.

---

5. Make sure the appropriate fabric is named on the **Zoning Policies** dialog box.
6. Perform one of the following actions based on the task you want to complete:
  - To enable the default zone, click **Enable**, and then click **OK**.
  - To disable the default zone, click **Disable**, and then click **OK**.
7. Click **OK** to apply your changes and close the **Zoning Policies** dialog box.
8. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

## Creating a zone alias

An alias is a logical group of port index numbers and WWNs. Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than inputting a long string of individual members. You can specify members of an alias using the following methods:

- Identifying members by switch domain and port index number pair (for example, 2, 20).
- Identifying members by device node and device port WWNs.

Zone aliases are supported only in Brocade Native mode (InteropMode 0) and in a mixed Fabric OS and M-EOS McDATA Fabric Mode (InteropMode 2).

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.

5. Click **New Alias**.

The **New Alias** dialog box displays.

6. Type the desired name for the alias in the **Alias Name** field.
7. Select **WWN** or **Domain, Port Index** to choose how to display the objects in the **Potential Members** list.
8. Show all discovered fabrics in the **Potential Members** list by right-clicking in the **Potential Members** list and selecting **Display All**.
9. Select one or more members that you want to add to the alias in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
10. Click the right arrow between the **Potential Members** list and **Selected Member(s)** list to add the selected members to the alias.
11. Click **OK** on the **New Alias** dialog box to save your changes.
12. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

### Editing a zone alias

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Select the alias you want to edit in the **Alias** list.
5. Click **Edit**.

The **Edit Alias** dialog box displays.

6. Add members to the alias by completing the following steps.
  - a. Select **WWN** or **Domain, Port Index** to choose how to display the objects in the **Potential Members** list.
  - b. Show all discovered fabrics in the **Potential Members** list by right-clicking in the **Potential Members** list and selecting **Expand All**.
  - c. Select one or more members that you want to add to the alias in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
  - d. Click the right arrow between the **Potential Members** list and **Selected Member(s)** list to add the selected members to the alias.
7. Remove members from the alias by completing the following steps.
  - a. Select one or more members that you want to remove from the alias in the **Selected Member(s)** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
  - b. Click the left arrow between the **Potential Members** list and **Selected Member(s)** list to remove the selected members to the alias.
8. Click **OK** on the **Edit Alias** dialog box to save your changes.
9. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

## Removing an object from a zone alias

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Show all objects in the **Alias** list by right-clicking a object and selecting **Tree > Expand All**.
5. Select one or more objects that you want to remove from the alias in the **Alias** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)  
You can select objects from different zone aliases.
6. Right-click one of the selected objects and select **Remove**.  
To selected objects are removed from the associated **Zone Alias**.
7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

## Exporting zone aliases

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Click **Export**.  
The **Export Alias** dialog box displays.
5. Browse to the location to which you want to export the zone alias data.
6. Enter a name for the export file in the **File Name** field.
7. Click **Export Alias**.
8. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

## Renaming a zone alias

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Right-click the zone alias you want to rename and select **Rename**.
5. Edit the name and press **Enter**.
6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

## Creating a zone configuration

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Click **New Config**.  
A new configuration displays in the **Zone Configs** list.
5. Enter a name for the zone configuration.  
For zone name requirements and limitations, refer to [“Zoning naming conventions”](#) on page 605.
6. Press **Enter**.  
Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the zone creation.
7. Add zones to the zone configuration.  
For step-by-step instructions, refer to [“Adding zones to a zone configuration”](#) on page 619.
8. Click **OK** or **Apply** to save your changes.  
A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Viewing zone configuration properties

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Potential Members** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
4. Right-click the zone configuration you want to review in the **Zone Configs** list and select **Properties**.  
The **Zone Config Properties** dialog box displays.

5. Review the zone configuration properties.

The following information is included in the zone properties:

- **Zone Config Name**—The name of the selected zone configuration.
- **Number of Zones**—The number of zones in the selected zone configuration.
- **Total Zone Members**—The total number of zone members in the selected zone configuration.
- **Unique Zone Members**—The total number of zone members that are unique in the zone configuration.
- **Status**—The status of the selected zone configuration (active or not active).

6. Click **OK** to close the **Zone Config Properties** dialog box.

## Adding zones to a zone configuration

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations to which you want to add zones in the **Zone Configs** list. (Press **SHIFT** or **CTRL** and click each zone configuration name to select more than one zone configuration.)
5. Select one or more zones to add to the zone configurations in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
6. Click the right arrow between the **Zones** list and **Zone Configs** list to add the zones to the zone configurations.
7. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Activating a zone configuration

For FC fabrics and router fabrics, when a zone configuration is active, its members can communicate with one another. Only one zone configuration can be active at any given time.

When you initiate activation of a zone configuration, a number of checks are performed on the zone configuration. These checks are performed before the **Activate Zone Config** dialog box is displayed, and look for the following problems:

- Zone and zone configuration name violations
- Zoning configuration violations
- Zone configuration change limit violations

For pure EOS fabrics, during zone configuration activation, the total number of zone members in each zone and in the zone configuration are checked against the limits imposed by the firmware and hardware product. If the limits are exceeded, a message is displayed informing you of the exceeded limits as well as the zone configuration failure information. Click **OK** to close the message box, and take appropriate action to meet the limits. For FC fabrics, this calculation is not done during activation, but a message is displayed whenever the size of the zone database exceeds the limits imposed by the switch.

When a zone configuration is activated, the entire zone database is sent to the fabric, except for McDATA Open Mode (Interop Mode 3) or a pure M-EOS fabric, when only the active configuration information is sent to the fabric.

---

### NOTE

Only one server should be run at a time (actual servers performing discovery) or logon conflicts may occur. Also, activation speeds may differ depending on the hardware vendor and type of zoning used.

---

There are several conditions that could cause the **Activate** button to be unavailable. They include the following:

- If you do not have access privileges to activate zone configurations, the **Activate** button on the **Zone DB** tab will be unavailable. You will not be able to activate a zone configuration unless your access privileges are redefined.
- The fabric is not manageable.
- You do not have Read/Write or Activate privileges for the selected fabric and the selected zone database (for FC fabric only).
- The selected fabric is not supported by the Management application.
- The selected fabric is no longer discovered.
- In McDATA Open Mode (InteropMode 3), the seed switch is a Fabric OS switch and either no EOS switch is in the fabric or none of the EOS switches are manageable.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone configuration you want to activate in the **Zone Configs** list.

5. Click **Activate**.

The Management application begins performing various checks. Note the following events that may occur:

- For FC fabrics, and depending on the characters included in the name you gave to this zone configuration, a message may display informing you the name contains characters that are not accepted by some switch vendors and asking whether you want to proceed. Click **Yes** to continue and proceed to the **Activate Zone Config** dialog box, or click **No** to cancel the activation and consider your naming options.
- For pure EOS fabrics, when the total number of zones and zone members defined exceeds the limit recommended for the system firmware, a warning message displays informing you of this fact and asking whether you want to proceed. Consider carefully whether you want to continue with the zone configuration activation. The limits are set to ensure stable fabrics; if you proceed, you may undermine the stability of your fabric. Click **Yes** to continue and proceed to the **Activate Zone Config** dialog box, or click **No** to cancel the activation.

You can then click **Cancel** to close the **Activate Zone Config** dialog box, reduce the number of zones or zone members on the **Zone DB** tab, and then return to this procedure to activate the zone configuration.

6. Review the information in the **Activate Zone Config** dialog box.

- a. Make sure the selected zone configuration is the one you want to activate.
- b. Select or clear the **Generate a report** check box as required.
- c. If you are activating a zone configuration from the offline zone database, select or clear the **Save only the selected zone configuration to the existing zone database in the fabric** check box.
  - If the check box is cleared (default), the entire offline zone database is saved to the switch and replaces the existing online zone database.
  - If the check box is selected, only the selected zone configuration and any TI zones in the offline zone database are saved to the switch and are added to the existing online zone database.

7. Click **OK** to activate the zone configuration.

If you are activating a zone configuration from the offline zone database, a message might display informing you of name conflicts between items in the offline zone database and the existing online zone database. Click **Yes** to overwrite the items in the online zone database, or **No** to cancel the activation.

A message box displays informing you that the zones and zone configurations you change will be saved in the zone database and asking whether you want to proceed. Click **Yes** to confirm the activation, or **No** to cancel the activation.

When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone configuration and its zones display green. When it fails, the message includes the reason for the failure.

8. Click **OK** to continue.

The **Activate Zone Config** dialog box is closed and the **Zone DB** tab displays.

9. Click **OK**.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

### Deactivating a zone configuration

Use this procedure to deactivate the active zone configuration.

There are several conditions that could cause the **Deactivate** button to be unavailable. They include the following:

- There is no active zone configuration in the selected fabric.
- The fabric is not manageable.
- You do not have Read/Write or Activate privileges for the selected fabric and the selected zone database (for FC fabric only).
- The selected fabric is not supported by the Management application.
- The selected fabric is no longer discovered.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Active Zone Config** tab.

3. Select an FC fabric from the **Active Zone Config** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **Deactivate**.

5. Click **Yes** on the confirmation message.

If the deactivation succeeded, the zone configuration no longer displays in the **Active Zone Config** tab.

If the deactivation failed, the zone configuration still displays in the **Active Zone Config** tab.

6. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Creating an offline zone database

Use this procedure to create a zone database and save it offline.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a zone database from the **Zone DB** list.
4. Select **Save As** from the **Zone DB Operation** list.

The **Save Zone DB As** dialog box displays.

5. Enter a name for the database in the **Zone DB Name** field.
6. Click **OK**.
7. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

8. If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
9. Create the desired zones.

For specific instructions, refer to [“Creating a new zone”](#) on page 608.

10. Add members to each zone.

For specific instructions, refer to [“Adding members to a zone”](#) on page 609 and [“Creating a new member in an LSAN zone”](#) on page 630.

11. Create a zone configuration.

For specific instructions, refer to [“Creating a zone configuration”](#) on page 618.

12. Activate the zone configuration.

For specific instructions, refer to [“Activating a zone configuration”](#) on page 620.

13. Set zoning policies, if necessary.

For specific instructions, refer to [“Enabling or disabling the default zone for fabrics”](#) on page 614 and [“Enabling or disabling safe zoning mode for fabrics”](#) on page 615.

14. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

### Refreshing a zone database

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a zone database from the **Zone DB** list.
4. Select **Refresh** from the **Zone DB Operation** list.

A message displays informing you that refresh will overwrite the selected database. Click **Yes** to continue.

5. Click **OK**.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

### Merging two zone databases

If a zone or zone configuration is merged, the resulting zone or zone configuration includes *all* members that were marked for addition or removal as well as all members not otherwise marked.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Select **Compare** from the **Zone DB Operation** list.

The **Compare/Merge Zone DBs** dialog box displays, as shown in [Figure 266](#).

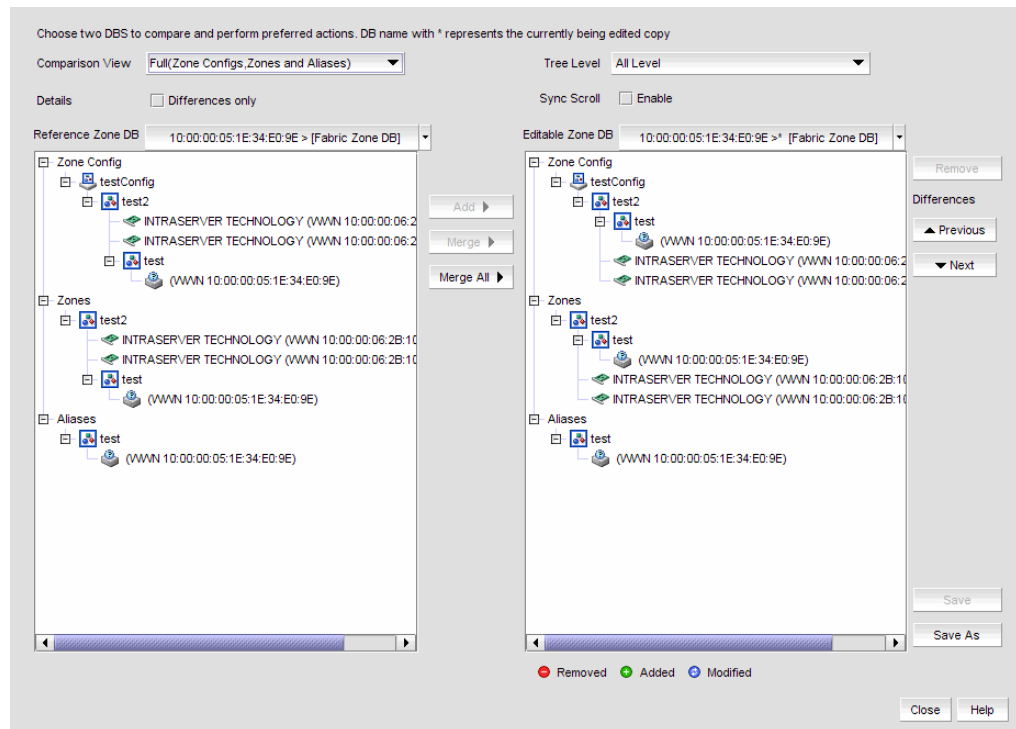


FIGURE 266 Compare/Merge Zone DBs dialog box

3. Select a database from the **Reference Zone DB** field.
4. Select a database from the **Editable Zone DB** field.

The **Reference Zone DB** and **Editable Zone DB** areas display all available element types (zone configurations, zones, and aliases) for the two selected zone databases. In the **Editable zone DB** area, each element type and element display with an icon indicator (Table 31) to show the differences between the two databases.

5. Set the display for the database areas by selecting one of the following from the **Comparison View** list:
  - **Storage-to-Host Connectivity**—Displays only storage and host devices.
  - **Host-to-Storage Connectivity**—Displays only host and storage devices.
  - **Full (Zone Configs, Zones, Aliases)**—Displays all zone configurations, zones, and aliases.
6. Set the level of detail for the database areas by selecting one of the following options from the **Tree Level** list.

---

#### NOTE

This list is only available when you set the **Comparison View** to **Full (Zone Configs, Zones, Aliases)**.

---

- **All Level**—Displays all zone configurations, zones, and aliases.
  - **Zone Configs**—Displays only zone configurations.
  - **Zones**—Displays only zones.
7. Select the **Differences** check box to display only the differences between the selected databases.

8. Select the **Sync Scroll Enable** check box to synchronize scrolling between the selected databases.
9. Merge zone configurations by completing the followings steps.
  - a. Select one or more zone configuration nodes from the **Reference Zone DB** area.
  - b. Select an element in the **Editable Zone DB** area.
  - c. Click **Merge**.
10. Merge zones by completing the followings steps.
  - a. Select one or more zones from the **Reference Zone DB** area.
  - b. Select one zone from the **Editable Zone DB** area.
  - c. Click **Merge**.
11. Merge aliases by completing the followings steps.
  - a. Select one or more aliases from the **Reference Zone DB** area.
  - b. Select one alias from the **Editable Zone DB** area.
  - c. Click **Merge**.
12. Merge all elements by clicking **Merge All**.
13. Add elements (aliases, zones, and zone configurations) to the editable database by completing the followings steps.
  - a. Select one or more of the same elements in the **Reference Zone DB** area.
  - b. Select the element type in the **Editable Zone DB** area.
  - c. Click **Add**.
14. Remove elements from the editable zone database by selecting an available element (added) from the Editable Zone DB are and clicking **Remove**.  
  
 Note that if a zone is removed from a zone configuration, it is removed *only* from that single zone configuration. However, if the zone is removed from the list of zones, it is removed from *all* zone configurations.
15. Click **Save As** to save the editable zone database in the offline repository.

### Saving a zone database to a switch

1. Select **Configure > Zoning > Fabric**.  
 The **Zoning** dialog box displays.
2. Select a zone database from the **Zone DB** list.
3. Select **Save to Switch** from the **Zone DB Operation** list.
4. Click **Yes** on the confirmation message.  
 The selected zone database is saved to the fabric without enabling a specific zone configuration.
5. Click **OK** to save your work and close the **Zoning** dialog box.

## Exporting an offline zone database

---

**NOTE**

You cannot export an online zone database.

---

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Select an offline zone database from the **Zone DB** list.
3. Select **Export** from the **Zone DB Operation** list.  
The **Export Zone DB** dialog box displays.
4. Browse to the location where you want to export the zone database file (.xml format).
5. Click **Export Zone DB**.
6. Click **OK** to save your work and close the **Zoning** dialog box.

## Importing an offline zone database

---

**NOTE**

You cannot import an online zone database.

---

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Select an offline zone database from the **Zone DB** list.
3. Select **Import** from the **Zone DB Operation** list.  
The **Import Zone DB** dialog box displays.
4. Browse to the zone database file (.xml format).
5. Click **Import Zone DB**.
6. Click **OK** to save your work and close the **Zoning** dialog box.

## Rolling back changes to the offline zone database

Use this procedure to reverse changes made to an offline zone database.

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Select the zone database you want to roll back from the **Zone DB** list.  
You must select an offline zone database that has a value in the **Last Saved to Fabric** column.  
You cannot roll back changes for zone databases that were never saved to the fabric.
3. Select **Roll Back** from the **Zone DB Operation** list.  
The selected zone database reverts back to what it was before the changes were applied.
4. Click **OK** to save your work and close the **Zoning** dialog box.

## LSAN zoning

LSAN zoning is available only for backbone fabrics and any directly connected edge fabrics. A backbone fabric is a fabric that contains an FC router. All discovered backbone fabrics have the prefix LSAN\_ in their fabric name, which is listed in the Zoning Scope list.

### Configuring LSAN zoning

The following procedure provides an overview of the steps you must perform to configure LSAN zoning.

Note that for any zoning-related procedure, changes to a zone database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box.

1. Select a backbone fabric from the Connectivity Map or Product List.
2. Select **Configure > Zoning > LSAN Zoning (Device Sharing)**.

The **Zoning** dialog box displays.

3. Click the **Zone DB** tab if that tab is not automatically displayed.
4. If you want to show all edge fabrics in your backbone fabric in the **Potential Members** list, right-click a device and select **Table > Expand All**.
5. Create the LSAN zones.

For specific instructions, refer to [“Creating a new LSAN zone”](#) on page 629.

6. Add members to each zone.

For specific instructions, refer to [“Adding members to the LSAN zone”](#) on page 629.

---

#### NOTE

You cannot add an LSAN zone to a zone configuration.

---

7. Click **Activate**.
- The **Activate LSAN Zones** dialog box displays.
8. Review the information in this dialog box.
9. Click **OK** to activate the LSAN zones and close the dialog box.

A message box displays informing you that the zones you change will be saved in the zone database and asking whether you want to proceed. Click **Yes** to confirm the activation, or **No** to cancel the activation.

When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone configuration and its zones display green. When it fails, the message includes the reason for the failure.

10. Click **OK** to continue.

All LSAN zones are activated on the selected fabrics and saved to the Zone DB.

11. Click **OK** to close the dialog box.

## Creating a new LSAN zone

1. Select a backbone fabric from the Connectivity Map or Product List.
2. Select **Configure > Zoning > LSAN Zoning (Device Sharing)**.  
The **Zoning** dialog box displays.
3. Click the **Zone DB** tab if that tab is not automatically displayed.
4. Click **New Zone**.  
The prefix LSAN\_ is automatically added in the text field.
5. Enter a name for the zone.  
For zone name requirements and limitations, refer to [“Zoning naming conventions”](#) on page 605.
6. Press **Enter**.  
Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the zone creation.
7. Click **Activate**.  
The **Activate LSAN Zones** dialog box displays.
8. Review the information in this dialog box.
9. Click **OK** to activate the LSAN zones.  
A message box displays informing you that the zones you change will be saved in the zone database and asking whether you want to proceed. Click **Yes** to confirm the activation, or **No** to cancel the activation.  
  
When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone configuration and its zones display green. When it fails, the message includes the reason for the failure.
10. Click **OK** to continue.  
All LSAN zones are activated on the selected fabrics and saved to the Zone DB.
11. Click **OK** to close the dialog box.

## Adding members to the LSAN zone

Use this procedure to add a member to an LSAN zone when the member is listed in the **Potential Members** list of the **Zone DB** tab.

1. Select a backbone fabric from the Connectivity Map or Product List.
2. Select **Configure > Zoning > LSAN Zoning (Device Sharing)**.  
The **Zone DB** tab of the **Zoning** dialog box displays.
3. If you want to show all discovered fabrics in the **Potential Members** list, right-click anywhere in the table and select **Display All**.

4. Select one or more LSAN zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
5. Select one or more members to add to the zone in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
6. Click the right arrow between the **Potential Members** list and **Zones** list to add the selected members to the zone.

A message may display informing you that one or some of the selected potential members cannot be zoned. Click **OK** to close the message box. Reconsider your selections and make corrections as appropriate.

7. Click **Activate**.

The **Activate LSAN Zones** dialog box displays.

8. Review the information in this dialog box.
9. Click **OK** to activate the LSAN zones.

A message box displays informing you that the zones you change will be saved in the zone database and asking whether you want to proceed. Click **Yes** to confirm the activation, or **No** to cancel the activation.

When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone configuration and its zones display green. When it fails, the message includes the reason for the failure.

10. Click **OK** to continue.

All LSAN zones are activated on the selected fabrics and saved to the Zone DB.

11. Click **OK** to close the dialog box.

## Creating a new member in an LSAN zone

Use this procedure to add a member to an LSAN zone when the member is not listed in the **Potential Members** list of the **Zone DB** tab.

For instructions to add a member to a zone when the member is listed in the **Potential Members** list, refer to the procedure [“Adding members to the LSAN zone”](#) on page 629.

1. Select a backbone fabric from the Connectivity Map or Product List.
2. Select **Configure > Zoning > LSAN Zoning (Device Sharing)**.
3. Select one or more zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
4. Click **New Member**.

The **Add Zone Member** dialog box displays.

5. Add the new member by port WWN by completing the following steps.
  - a. Select the **End Device Port WWN** option.
  - b. Enter a port WWN in the **End Device Port WWN** field.  
If you enter a WWN that has been used by a discovered device, a message displays informing you of this and instructing you to enter a port WWN. Click **OK** to close the message box and enter an appropriate WWN.
  - c. (Optional) Click the **Assign Name** check box and enter a name in the field.  
If a name was previously assigned, the name appears in the field and a message displays asking whether you want to overwrite the existing name. Click **Yes** to continue and assign a new name, or **No** to decline and close the message box.
6. Click **OK** to save your changes and close the **Add Zone Member** dialog box.  
OR  
Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat steps 3 through 5 as many times as needed, and proceed to step 6 when you have finished adding members.
7. Click **Activate**.  
The **Activate LSAN Zones** dialog box displays.
8. Review the information in this dialog box.
9. Click **OK** to activate the LSAN zones.  
A message box displays informing you that the zones you change will be saved in the zone database and asking whether you want to proceed. Click **Yes** to confirm the activation, or **No** to cancel the activation.  
  
When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone configuration and its zones display green. When it fails, the message includes the reason for the failure.
10. Click **OK** to continue.  
All LSAN zones are activated on the selected fabrics and saved to the Zone DB.
11. Click **OK** to close the dialog box.

## Activating LSAN zones

1. Select a backbone fabric from the Connectivity Map or Product List.
2. Select **Configure > Zoning > LSAN Zoning (Device Sharing)**.  
The **Zone DB** tab of the **Zoning** dialog box displays.
3. Click **Activate**.  
The **Activate LSAN Zones** dialog box displays.
4. Review the information in this dialog box.

5. Click **OK** to commit the LSAN zones and activate them in the selected fabrics.

A message box displays informing you that the zones you change will be saved in the zone database and asking whether you want to proceed. Click **Yes** to confirm the activation, or **No** to cancel the activation.

When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone configuration and its zones display green. When it fails, the message includes the reason for the failure.

6. Click **OK** to close the dialog box.

If you click OK without having activated the LSAN zones, a message displays informing you that your changes will be lost.

## Traffic isolation zoning

A Traffic Isolation zone (TI zone) is a special zone that isolates inter-switch traffic to a specific, dedicated path through the fabric. A TI zone contains a list of E\_Ports, followed by a list of N\_Ports. When the TI zone is activated, the fabric attempts to isolate all inter-switch traffic between N\_Ports to only those E\_Ports that have been included in the zone. The fabric also attempts to exclude traffic not in the TI zone from using E\_Ports within that TI zone.

Traffic isolation zoning is only supported with domain and port index number members.

A TI zone can have failover enabled or disabled.

Disable failover if you want to guarantee that TI zone traffic uses only the dedicated path, and that no other traffic can use the dedicated path.

Enable failover if you want traffic to have alternate routes if either the dedicated or non-dedicated paths cannot be used.

---

### ATTENTION

If failover is disabled, use care when planning your TI zones so that non-TI zone devices are not isolated. If disabled failover is not used correctly, it can cause major fabric disruptions that are difficult to resolve.

---

## Enhanced TI zones

In Fabric OS 6.4.0 or higher, ports can be in multiple TI zones. Zones with overlapping port members are called *enhanced TI zones* (ETIZ).

Enhanced TI zones are supported only on the following platforms:

- 24-port, 8 Gbps FC Switch
- 40-port, 8 Gbps FC Switch
- 80-port, 8 Gbps FC Switch
- 8 Gbps 12-port Embedded Switch
- 8 Gbps 24-port Embedded Switch
- 8 Gbps 16-port Embedded Switch
- 8 Gbps 24-port Embedded Switch

- 8 Gbps 16-FC ports, 6-Gbit ports Extension Switch
- 24 - 8 Gbps FC Port, 8 - 10 Gbps CEE Port Switch
- 8 Gbps 40-port Switch
- 384-port Backbone Chassis
- 192-port Backbone Chassis
- 8 Gbps Encryption Switch

Enhanced TI zones are supported only if the following conditions are met:

- Every switch must be one of the supported platforms, as listed above.
- Every switch must be running Fabric OS v6.4.0 or later.

If the fabric contains a switch running an earlier version of Fabric OS, you cannot create an enhanced TI zone.

The failover mode must be the same for each enhanced TI zone to which a port belongs.

You cannot merge a downlevel switch into a fabric containing enhanced TI zones, and you cannot merge a switch with enhanced TI zones defined into a fabric containing switches that do not support ETIZ.

---

**NOTE**

FC router domains and EOS switches are excluded from the ETIZ platform restrictions. You can create enhanced TI zones with these switches in the fabric.

---

## Configuring traffic isolation zoning

The following procedure provides an overview of the steps you must perform to configure traffic isolation zoning.

Note that for any zoning-related procedure, changes to a zone database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box. If you click **Cancel** or the close button (X), no changes are saved.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select **Domain**, **Port Index** from the **Type** list.
5. If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
6. Create the traffic isolation zones.

For specific instructions, refer to [“Creating a traffic isolation zone”](#) on page 634.

7. Add members to each zone.

For specific instructions, refer to [“Adding members to a traffic isolation zone”](#) on page 635.

---

**NOTE**

You cannot add a traffic isolation zone to a zone configuration.

---

8. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zones are activated when you activate a zone configuration in the same zone database.

### Creating a traffic isolation zone

Traffic isolation zones are configurable only on a Fabric OS device. The seed switch must be running Fabric OS 6.1.1 or later.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select **Domain, Port Index** from the **Type** list.
5. Select **New TI Zone** from the **New Zone** list.
6. Enter a name for the zone.

For zone name requirements and limitations, refer to [“Zoning naming conventions”](#) on page 605.

7. Press **Enter**.

Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the zone creation.

8. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Adding members to a traffic isolation zone

---

### NOTE

Traffic isolation zones are configurable only on a Fabric OS device.

---

Use this procedure to add a member to a zone when the member is listed in the **Potential Members** list of the **Zone DB** tab. Only ports can be added as members to a traffic isolation zone. You must add two or more N\_Ports as well as all E\_Ports on the path between the N\_Ports.

---

### NOTE

You cannot add a device as a member to a traffic isolation zone.

---

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
  2. Click the **Zone DB** tab if that tab is not automatically displayed.
  3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
  4. If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
  5. Select one or more traffic isolation zones to which you want to add members in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
  6. Select **Domain, Port Index** from the **Type** list.
  7. Select two or more N\_Ports (as well as all E\_Ports on the path between the N\_Ports) to add to the zone in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each port to select more than one port.)
- 

### NOTE

TI zones can be created in fabrics that contain logical switches; however, you can only select physical ports for TI zones.

---

If you select a trunk port to add to the TI zone, all trunk ports in the trunk group are added to the TI zone automatically.

8. Click the right arrow between the **Potential Members** list and **Zones** list to add the selected ports to the zone.

A message may display informing you that one or some of the selected potential members cannot be zoned. Click **OK** to close the message box. Reconsider your selections and make corrections as appropriate.

9. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Enabling a traffic isolation zone

---

**NOTE**

Traffic isolation zones are configurable only on a Fabric OS device.

---

Use this procedure to enable a traffic isolation zone. When a zone configuration in the same zone database is activated, the enabled TI zones are also activated at that time. Traffic isolation zones are enabled by default when you create them.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to enable in the **Zones** list and select **Configured Enabled**.

5. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zone is activated when you activate a zone configuration in the same zone database.

## Disabling a traffic isolation zone

---

**NOTE**

Traffic isolation zones are configurable only on a Fabric OS device.

---

Traffic isolation zones are enabled by default when you create them. Use this procedure to disable a traffic isolation zone. To apply the settings and deactivate the zone, you must activate a zone configuration in the same zone database.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to disable in the **Zones** list and clear the **Configured Enabled** check box.

5. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zone is not disabled until you activate a zone configuration in the same zone database.

## Enabling failover on a traffic isolation zone

---

### NOTE

Traffic isolation zones are configurable only on a Fabric OS device.

---

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Right-click the traffic isolation zone you want to enable failover on in the **Zones** list and select **Configured Failover**.
5. Click **OK** or **Apply** to save your changes.  
A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Disabling failover on a traffic isolation zone

---

### NOTE

Traffic isolation zones are configurable only on a Fabric OS device.

---

If failover is disabled, be aware of the following considerations:

- Ensure that there are non-dedicated paths through the fabric for all devices that are not in a TI zone.
- If you create a TI zone with just E\_Ports, failover must be enabled. If failover is disabled, the specified ISLs will not be able to route any traffic.
- Ensure that there are multiple paths between switches. Disabling failover locks the specified route so that only TI zone traffic can use it.

---

### ATTENTION

If failover is disabled, use care when planning your TI zones so that non-TI zone devices are not isolated. If disabled failover is not used correctly, it can cause major fabric disruptions that are difficult to resolve.

---

You cannot disable failover if the TI zone was created in the base fabric or in a fabric in which a logical switch is configured to use XISLs (the **Base Fabric for Transport** check box is selected).

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

- 4. Right-click the traffic isolation zone you want to disable failover on in the **Zones** list and clear the **Configured Failover** check box.
- 5. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.




## Zoning administration

This section provides instructions for performing administrative functions with zoning. You can rename, duplicate, delete, and perform other tasks on zone members, zones, and zone configurations.

### Comparing zone databases

You can compare zone databases against one another to identify any and all differences between their membership prior to sending them to the switch. Once the two databases have been compared, icons display to show the differences between the two databases. These icons are illustrated and described in [Table 31](#).

**TABLE 31** Compare icon indicators

| Icon                                                                                | Description                                                             |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
|  | Added—Displays when an element is added to the editable database.       |
|  | Modified—Displays when an element is modified on the editable database. |
|  | Removed—Displays when an element is removed from the editable database. |

To compare two zone databases, complete the following steps.

- 1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
- 2. Select **Compare** from the **Zone DB Operation** list.  
The **Compare/Merge Zone DBs** dialog box displays, as shown in [Figure 267](#).

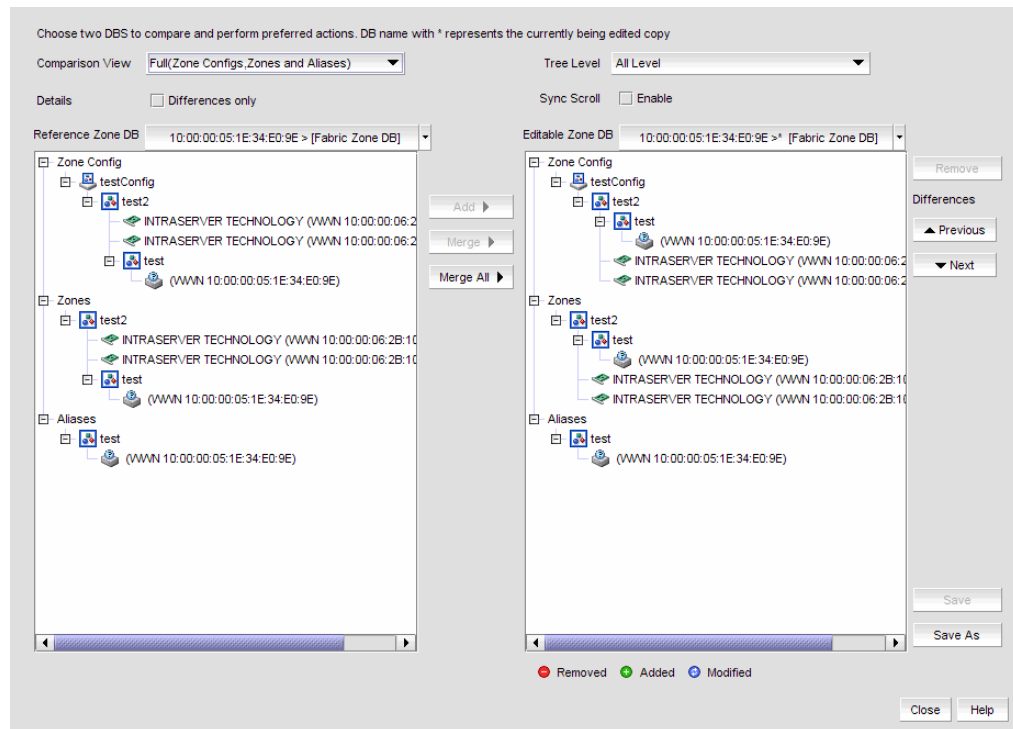


FIGURE 267 Compare/Merge Zone DBs dialog box

3. Select a database from the **Reference Zone DB** field.
4. Select a database from the **Editable Zone DB** field.

The **Reference Zone DB** and **Editable Zone DB** areas display all available element types (zone configurations, zones, and aliases) for the two selected zone databases. In the **Editable zone DB** area, each element type and element display with an icon indicator (Table 31) to show the differences between the two databases.

5. Set the display for the database areas by selecting one of the following from the **Comparison View** list:
  - **Storage-to-Host Connectivity**—Displays only storage and host devices.
  - **Host-to-Storage Connectivity**—Displays only host and storage devices.
  - **Full (Zone Configs, Zones, Aliases)**—Displays all zone configurations, zones, and aliases.
6. Set the level of detail for the database areas by selecting one of the following options from the **Tree Level** list.

---

#### NOTE

This list is only available when you set the **Comparison View** to **Full (Zone Configs, Zones, Aliases)**.

---

- **All Level**—Displays all zone configurations, zones, and aliases.
  - **Zone Configs**—Displays only zone configurations.
  - **Zones**—Displays only zones.
7. Select the **Differences** check box to display only the differences between the selected databases.

8. Select the **Sync Scroll Enable** check box to synchronize scrolling between the selected databases.
9. Click **Previous** or **Next** to navigate line-by-line in the **Editable Zone DB** area.
10. Click **Close**.

To merge two zone databases, refer to [“Merging two zone databases”](#) on page 624.

## Managing zone configuration comparison alerts

You can turn off the automatic zone configuration comparison function if you no longer want to see two of the alert messages that the comparison can produce. When a zone configuration is successfully activated, the comparison function can display an alert icon if either of two conditions exist.

The messages in question are “The active zone configuration does not exist in the zone database” and “The active zone configuration does not match <zone configuration> in the zone database.” To turn off the icons and the messages, complete the following steps.

1. After successfully activating a zone configuration, click the **Active Zone Config** tab.
2. Select the check box labeled **Turn off the comparison alerts between the active zone config and the zone database**.

Any existing alert icons and messages are cleared and further comparisons are prevented.

The check box selection defaults to the last setting per user.

## Setting change limits on zoning activation

Use this procedure to set a limit on the number of changes a user can make to the zone database before activating a zone configuration. If the user exceeds the limit, zone configuration activation is not allowed. By default, all fabrics allow unlimited changes. Changes include adding, removing, or modifying zones, aliases, and zone configurations.

Using the following procedure you can do the following:

- Set a different limit for each fabric.
- Set limits on some fabrics while allowing other fabrics to have unlimited changes.
- Set a limit for fabrics that will be discovered later.

---

### NOTE

You must have the Zoning Set Edit Limits privilege to perform this task.

---

1. Select **Configure > Zoning > Set Change Limits**.  
The **Set Change Limits for Zoning Activation** dialog box displays.
2. Click **Change Count** for the fabric on which you want to set limits.  
The field changes to an editable field.
3. Enter the maximum number of zone database changes that can be made for that fabric before a zone configuration is activated.  
To set a limit, enter a positive integer.  
To allow unlimited changes, enter 0.

4. Repeat [step 2](#) and [step 3](#) for each fabric on which you want to set limits.
5. To set a limit for new, undiscovered fabrics, enter a value in the **Default Change Count for New Fabrics** field.  
The default value is 0 (Unlimited).
6. Select the **Enforce change limits during zone activation** check box to enforce the change limits.  
If you want to set the limits now, but turn on enforcement of the limits at a later time, make sure the check box is clear.
7. Click **OK** to save your changes and close the dialog box.

## Deleting a zone

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Select one or more zones in the **Zones** list that you want to delete, then right-click and select **Delete**.  
A message box displays asking you to confirm the deletion.
5. Click **Yes** to delete the selected zone.  
The message box closes and, if successful, the zone or zones are removed from the **Zones** list.

---

### NOTE

If you delete something in error, click **Cancel** on the **Zoning** dialog box to exit without saving changes since the last operation (**Apply** or **Activate**). When you reopen the dialog box, the zone is restored.

---

6. Click **OK** or **Apply** to save your changes.  
A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Deleting a zone alias

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Right-click the zone alias you want to delete and select **Delete**.

5. Click **Yes** on the confirmation message.  
The selected zone alias is deleted from the **Alias** list.
6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

### Deleting a zone configuration

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Select one or more zone configurations in the **Zone Configs** list that you want to delete, then right-click and select **Delete**.  
A message box displays asking you to confirm the deletion.
5. Click **Yes** to delete the selected zone configuration.  
The message box closes and, when successful, the selected zone configurations are removed from the **Zone Configs** list.

---

#### NOTE

If you select “**Do not show me this again.**” on the confirmation message box, the next time you delete a zone configuration, it will be deleted without requesting confirmation from you. If you delete something in error, click **Cancel** on the **Zoning** dialog box to exit without saving changes since the last operation (**Apply** or **Activate**). When you reopen the dialog box, the zone configuration is restored.

---

6. Click **OK** or **Apply** to save your changes.  
A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

### Deleting an offline zone database

For pure EOS fabrics in McDATA Fabric Mode (InteropMode 2) or McDATA Open Mode (InteropMode 3) and for mixed Fabric OS and M-EOS fabrics in McDATA Open Mode, you cannot delete the last available offline zone database, because only offline zoning is supported for these fabrics.

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning databases for the selected entity.

3. Select the offline zone database you want to delete in the **Zone DB** list.

---

**NOTE**

Only offline databases can be deleted.

---

4. Select **Delete** from the **Zone DB Operation** list.
5. Click **Yes** on the confirmation message.  
The message box closes and, when successful, the selected zone configurations are removed from the **Zone Configs** list.
6. Click **OK** to save your work and close the **Zoning** dialog box.  
A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Clearing the fabric zone database

---

**ATTENTION**

Clearing the zone database removes all zoning configuration information, including all aliases, zones, and zone configurations, in the fabric.

Clearing the fabric zone database is disruptive to the fabric.

---

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning databases for the selected entity.
3. Select the Fabric Zone DB from the **Zone DB** list.
4. Select **Clear All** from the **Zone DB Operation** list.
5. Click **Yes** on the confirmation message.  
The message box closes and, when successful, the Fabric Zone DB is cleared of all zoning configurations.
6. Click **OK** to close the **Zoning** dialog box.

## Removing all user names from a zone database

Use this procedure to remove all user names from the selected offline zone database.

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning databases for the selected entity.

3. Select a zone database that you have checked out (your user name is in the **Current User** column) in the **Zone DB** list.
4. Select **Undo CheckOut** from the **Zone DB Operation** list.
5. Click **Yes** in the confirmation message.  
This removes the user names of users currently logged in to the client from the **Current User** column for this zone database.
6. Click **OK** to save your work and close the **Zoning** dialog box.  
A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

### Duplicating a zone

When you duplicate a zone, you make a copy of it in the same zone database. The first time a zone is duplicated, the duplicate is automatically given the name `<zonelabel>_copy`. On subsequent times, a sequential number is assigned to the zone name, such as `<zonelabel>_copy_1`, `<zonelabel>_copy_2`, and `<zonelabel>_copy_3`.

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Select one or more zones in the **Zones** list that you want to duplicate, then right-click and select **Duplicate**.  
The duplicated zone or zones display in the **Zones** list.
5. (Optional) Type a new name for the zone.  
If you key in a new name, press **Enter** to save the name.  
Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the renaming. (For zone name requirements and limitations, refer to [“Zoning naming conventions”](#) on page 605.)
6. Click **OK** or **Apply** to save your changes.  
A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Duplicating a zone alias

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Right-click the zone alias you want to duplicate and select **Duplicate**.  
The duplicated zone alias displays in the **Alias** list (for example, <Zone\_Alias>\_Copy).
5. Edit the name.  
To edit the name, refer to [“Renaming a zone alias”](#) on page 617.
6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

## Duplicating a zone configuration

When you duplicate a zone configuration, you make a copy of it in the same zone database. The first time a zone configuration is duplicated, the duplicate is automatically given the name <zonesetlabel>\_copy. On subsequent times, a sequential number is assigned to the zone name, such as <zonesetlabel>\_copy\_1, <zonesetlabel>\_copy\_2, and <zonesetlabel>\_copy\_3.

Note that these naming conventions apply both to duplicate and deep duplicate operations.

1. Select **Configure > Zoning > Fabric**.  
The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Select one or more zone configurations in the **Zone Configs** list that you want to duplicate, then right-click and select one of the following options:
  - **Duplicate** - To duplicate the zone configuration or configurations.
  - **Deep Duplicate** - To duplicate the zone configuration or configurations *and* all included zones.
 The duplicated zone configuration or sets display in the **Zone Configs** list.
5. (Optional) Type a new name for the zone configuration.  
If you key in a new name, press **Enter** to save the name.  
Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the renaming. (For zone configuration name requirements and limitations, refer to [“Zoning naming conventions”](#) on page 605.)
6. Click **OK** or **Apply** to save your changes.  
A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Finding a member in one or more zones

Use this procedure to locate all instances of a member in the **Zones** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all fabrics discovered in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.

5. Select the device or port you want to find in the **Potential Members** list.

Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

6. Click **Find >** between the **Potential Members** list and **Zones** list.
  - If the member is found, all instances of the zone member found are highlighted in the **Zones** list.
  - If the member is not found, a message displays informing you of this. Click **OK** to close the message box.

## Finding a zone member in the potential member list

Use this procedure to locate a zone member in the **Potential Members** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone member in the **Zones** list that you want to find in the **Potential Members** list.

Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. Click **Find <** between the **Potential Members** list and the **Zones** list.
  - If the member is found, it is highlighted in the **Potential Members** list.
  - If the member is not found, a message displays informing you of this. Click **OK** to close the message box.
  - If there are no ports listed in the **Potential Members** list, a message displays informing you that additional action is required. Right-click within the list panel and select **Port Display** from the shortcut menu to display ports.

## Finding zones in a zone configuration

Use this procedure to locate all instances of a zone in the **Zone Configs** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone you want to find in the **Zones** list.

Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. Click **Find >** between the **Zones** list and the **Zone Configs** list.
  - If the zone is found, all instances of the zone are highlighted in the **Zone Configs** list.
  - If the zone is not found, a message displays informing you of this. Click **OK** to close the message box.

## Finding a zone configuration member in the zones list

Use this procedure to locate a zone configuration member in the **Zones** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone configuration member (i.e., the zone) in the **Zone Configs** list that you want to find in the **Zones** list.

Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. Click **Find <** between the **Zones** list and the **Zone Configs** list.
  - If the zone is found, it is highlighted in the **Zones** list.
  - If the zone is not found, a message displays informing you of this. Click **OK** to close the message box.

## Listing zone members

Use this procedure to identify the zone in the active zone configuration of the fabric to which an individual port belongs and the members of that zone.

Note that the procedure is performed from the main view of the Management application.

1. On the product device list of the Management application, expand the list of products to show the ports.
2. Select a port and select **Configure > List Zone Members**.  
 If the port is not a member of a zone, a message displays informing you of this. Click **OK** to close the message.  
 If the port is a member of a zone, the **List Zone Members** dialog box displays. The fabric's name, the port's name, and the WWN zone members display.
3. Click **Close** to exit the **List Zone Members** dialog box.

## Removing a member from a zone

Use the following procedure to remove one or more members from a zone or zones. Note that the member is not deleted; it is only removed from the zone.

1. Select **Configure > Zoning > Fabric**.  
 The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
 This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Click the plus sign (+) by the appropriate zone in the **Zones** list to expand the listing and show the zone's members.
5. Perform one of the following actions:
  - Right-click the name of the zone member you want to remove in the **Zones** list and select one of the following options from the shortcut menu that displays:
    - **Remove** - To remove the zone member from the selected zone.
    - **Remove All** - To remove the zone member from all zones to which it belongs.
  - To remove multiple zone members, select the members to be removed from the zone, and click the left arrow between the **Potential Members** list and the **Zones** list.

When successful, the zone member is removed from the **Zones** list.

6. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Removing a zone from a zone configuration

Use the following procedure to remove a zone from a zone configuration. Note that the zone is not deleted; it is only removed from the zone configuration.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.  
This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Click the plus sign (+) by the appropriate zone configuration in the **Zone Configs** list to expand the listing and show the zone configuration members.
5. Perform one of the following actions:

- Right-click the name of the zone you want to remove in the **Zone Configs** list and select **Remove**.
- To remove multiple zones, select the zones to be removed from the zone configuration, and click the left arrow between the **Zones** list and the **Zone Configs** list.

When successful, the zone is removed from the **Zone Configs** list.

6. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Removing an offline device

The Management application enables you to remove an offline device from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

3. Select **Offline Utility** from the **Zone DB Operation** list.

The **Offline Device Management** dialog box displays.

4. Select the check box for the offline device you want to remove in the **Remove** column.

Select the **Remove** check box to select all offline devices.

5. Click **OK** on the **Offline Device Management** dialog box.

A warning message displays informing you that the selected zone members will be replaced from all zones and aliases in the selected zone DB.

6. Click **OK** on the message.

7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

### Renaming a zone

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the name of the zone you want to change in the **Zones** list and select **Rename**.

5. Type the new name for the zone.

For zone name requirements and limitations, refer to [“Zoning naming conventions”](#) on page 605.

6. Press **Enter** to save the new name.

For FC fabrics, if an invalid name is entered for a zone or zone configuration, the application displays a warning message. If there is a naming violation according to the vendor, the switch returns the error message for the exact information along with the zone configuration activation failure message.

7. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

### Renaming a zone configuration

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the name of the zone configuration you want to change in the **Zone Configs** list and select **Rename**.

5. Type the new name for the zone configuration.

For zone configuration name requirements and limitations, refer to [“Zoning naming conventions”](#) on page 605.

6. Press **Enter** to save the new name.

Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the renaming and consider your options.

7. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Replacing zone members

A zone member can be replaced in a specific, selected zone, or, if it is the member of more than one zone, it can be replaced in all the zones to which it belongs.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the zone member you want to replace in the **Zones** list and select one of the following options from the shortcut menu that displays:

- **Replace** - To replace the zone member in a selected zone.
- **Replace All** - To replace all instances of the selected zone member.

When you select **Replace**, the **Replace Zone Member** dialog box displays. When you select **Replace All**, the same dialog box displays, but with the title **Replace Zone Member (all instances)**.

5. Select the option from the **Type** list that you want to use to identify the replacement zone member.
6. Enter the WWN, name, domain and port index numbers, or alias—whichever is appropriate for the method you chose in step 4.

When you choose the WWN method, the **Assign Name** field is available; you may define a name for the replacement zone member. If a name was previously assigned to the potential member, a message displays informing you of this and asking whether you want to overwrite the existing name. Click **Yes** to continue and assign a new name, or **No** to decline and dismiss the message box.

7. Click **OK**.

If you have entered more than one port name or zoning method, a message displays informing you of the error. Click **OK** to close the message, correct your entry, and click **OK** again.

If no entry error was made, the new zone member replaces the old zone member in the **Zones** list and the **Replace Zone Member** dialog box closes.

8. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

### Replacing an offline device by WWN

The Management application enables you to replace an offline device by WWN from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

3. Select **Offline Utility** from the **Zone DB Operation** list.

The **Offline Device Management** dialog box displays.

4. Make sure the **Remove** column check box, for the offline device you want to replace, is clear.

5. Select **WWN** (default) in the corresponding **Replace Using** list.

6. Enter the WWN or select the name of the offline device in the corresponding **Replace Using** field.

If the selected name has multiple device or device port WWNs assigned (names are set to non-unique in Management application), the **Device or Device Port WWN of Non-unique Name** dialog box displays. The WWN list includes all device and device port WWNs assigned to the selected name.

7. Click **OK** on the **Offline Device Management** dialog box.

A warning message displays informing you that the selected zone members will be removed from all zones and aliases in the selected zone DB.

8. Click **OK** on the message.

9. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## Replacing an offline device by name

The Management application enables you to replace an offline device by name from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

The **Zoning** dialog box displays.

2. Select an FC fabric from the **Zoning Scope** list.

This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

3. Select **Offline Utility** from the **Zone DB Operation** list.

The **Offline Device Management** dialog box displays.

4. Make sure the **Remove** column check box, for the offline device you want to replace, is clear.

5. Select **Name** (default is WWN) in the corresponding **Replace Using** list.

6. Select the name of the offline device in the corresponding **Replace Using** list.

If the selected name has multiple device or device port WWNs assigned (names are set to non-unique in Management application), the **Device or Device Port WWN of Non-unique Name** dialog box displays. The WWN list includes all device and device port WWNs assigned to the selected name.

7. Select the WWN you want to use from the **WWN** list and click **OK**.

8. Click **OK** on the **Offline Device Management** dialog box.

A warning message displays informing you that the selected zone members will be removed from all zones and aliases in the selected zone DB.

9. Click **OK** on the message.

10. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

## 22 Replacing an offline device by name

# Troubleshooting

---

## In this chapter

|                                                   |     |
|---------------------------------------------------|-----|
| • FC troubleshooting .....                        | 655 |
| • IP troubleshooting .....                        | 659 |
| • Client browser troubleshooting .....            | 663 |
| • Fabric tracking troubleshooting .....           | 663 |
| • FICON troubleshooting .....                     | 664 |
| • Launch Client troubleshooting .....             | 665 |
| • Performance troubleshooting .....               | 667 |
| • Port Fencing troubleshooting .....              | 671 |
| • Server Management Console troubleshooting ..... | 672 |
| • Supportsave troubleshooting .....               | 673 |
| • View All list troubleshooting .....             | 674 |
| • Zoning troubleshooting .....                    | 674 |

## FC troubleshooting

---

### NOTE

FC troubleshooting is only available for Fabric OS devices.

---

You can perform the following operations using FC troubleshooting:

- Trace Route (Path Information and FC Ping) – Use to obtain the detailed routing information for any two selected device ports. The devices can exist in the same fabric or in two different fabrics shared through FC Routers.
- Device Connectivity Troubleshooting – Use to identify any problems that might be preventing communication between the two selected device ports. The device ports can be selected from the same fabric or from two different fabrics.
- Fabric Device Sharing Diagnosis (pure Fabric OS fabrics only) – Use to confirm that any two or more selected fabrics are capable of sharing devices between them.

## Tracing FC routes

The Management application enables you to select a source port and a destination port and displays the detailed routing information from the source port or area on the local switch to the destination port or area on another switch.

Trace route cannot be performed on the offline devices or virtual devices.

---

### NOTE

Trace route is only supported on Fabric OS switches running Fabric OS 5.2 or later.

---

To trace routes, complete the following steps.

1. Select **Configure > FC Troubleshooting > Trace Route**.

The **Trace Route** dialog box displays.

2. Choose from one of the following options:

- Select a fabric from the **Fabric** list.
- Select a router from the **Routing** list. Requires Fabric OS 6.2 or later.

3. Select the source and destination ports by choosing one of the following:

The source and destination ports must be on the same fabric; however, they cannot be connected to the same switch.

- To enter the ports, select the **Enter port FC Address** option.
  - a. Enter the source port FC address in the **Source** field.
  - b. Enter the destination port FC address in the **Destination** field.
- To select the ports, select the **Select two device ports** option.
  - a. Right-click a fabric in the **Available Device Ports** table and select **Expand All**.
  - b. Select the ports (two) for which you want to display the detailed routing information from the **Available Device Ports** table.

4. Click the right arrow button.

5. Click **OK**.

The **Trace Route Summary** dialog box displays. This dialog box includes the following information:

- **Trace Route Summary.** This table shows a brief summary of the trace including the port WWN, port name, FC address, switch name, whether ping was successful, round trip time (minimum, maximum, and average) and whether the device ports are in active zones.
- **Forward Route.** This tab shows the path taken by data packets from the port belonging to the switch on which the trace route has been invoked (source port) to the port on the other switch (destination port).

- **Reverse Route.** This tab shows the path from the destination port to the source port.

---

**NOTE**

This reverse route may sometimes be different from the forward route.

---

- **FC Ping.** This tab shows the minimum, maximum and average round trip times between the selected device port WWNs and the domain controller. It details whether the selected device port WWNs are zoned or not. It also shows the number of frames sent to the device port, frames rejected, frames timed-out and frames received by the device port.

6. Click **Close** on the **Trace Route Summary** dialog box.
7. Click **Cancel** on the **Trace Route** dialog box.

## Troubleshooting device connectivity

To troubleshoot device connectivity, complete the following steps.

1. Select **Configure > FC Troubleshooting > Device Connectivity**.

The **Device Connectivity Troubleshooting** dialog box displays.

2. Select the source and destination ports on which you want to troubleshoot device connectivity using one of the following options:
  - Enter the source and destination ports directly by selecting the **Enter port FC Address** option and completing the following steps.
    - a. Enter the source port in the **Source** field.
    - b. Enter the destination port in the **Destination** field.
    - c. Click **Search and Add**.
  - Select the source and destination ports from a list by selecting the **Select two device ports** option and completing the following steps.
    - a. Right-click a fabric in the **Available Device Ports** table and select **Expand All**.
    - b. Select the ports (source and destination) for which you want to confirm device sharing from the **Available Device Ports** table.  
To add a detached device to troubleshoot device connectivity, refer to [“Adding a detached device”](#) on page 658.
    - c. Click the right arrow button.

3. Click **OK**.

The following diagnostic tests are performed:

- Device Status
- Switch port health status
- Zone configuration in the fabric
- LSAN zone configuration in edge fabrics
- Edge fabric - FC router physical connection status.
- Active ACL DCC policy check (Fabric OS only)

The **Device Connectivity Troubleshooting Results** dialog box displays.

If no problems are found, the diagnostic test is marked with a check mark. If problems are found, an alert icon appears next to the test, with a brief statement detailing the error as well as a suggested resolution.

4. Click **Re-run Diagnosis** to run the device connectivity on the same ports.
5. Click **Trace Route** to trace the route between the two selected ports.
6. Click **Close** on the **Device Connectivity Troubleshooting Results** dialog box.

### *Adding a detached device*

To add a detached device to the **Selected Device Ports** table, complete the following steps.

1. Select **Configure > FC Troubleshooting > Device Connectivity**.  
The **Device Connectivity Troubleshooting** dialog box displays.
2. Click **Add Detached**.
3. Enter the port WWN of the detached device port in the **Port WWN** field.
4. Click **OK**.

## Confirming fabric device sharing

---

### **NOTE**

Fabric device sharing is only available on pure Fabric OS fabrics.

---

To confirm fabric device sharing, complete the following steps.

1. Select **Configure > FC Troubleshooting > Fabric Device Sharing**.  
The **Fabric Device Sharing Diagnosis** dialog box displays.
2. Select the fabrics (two or more) for which you want to confirm device sharing from the **Available Fabrics** table.
3. Click the right arrow button.

4. Click **OK**.

The following checks are performed on the selected fabrics:

- Are the selected fabrics configured with an FC Router?
- Are the selected fabrics connected to the same backbone fabric?
- Is sharing of devices between backbone and edge fabric supported?

The **Fabric Device Sharing Diagnosis Results** dialog box displays with the details of the fabrics selected for diagnosis, the details of the tests performed, the results of the test, as well as short description of the test results.

5. Click **Close** on the **Fabric Device Sharing Diagnosis Results** dialog box.
6. Click **Cancel** on the **Fabric Device Sharing Diagnosis** dialog box.

## IP troubleshooting

---

### NOTE

IP troubleshooting is only available for Fabric OS devices.

---

You can perform the following operations using IP troubleshooting:

- **Ping.** Use to confirm that the configured FCIP tunnels are working correctly.
- **Trace Route.** Use to view the route information from a source port on the local device to a destination port on another device and determine where connectivity is broken.
- **Performance.** Select to view FCIP tunnel performance between two devices.

## Configuring IP ping

---

### NOTE

IP Ping only supported on Fabric OS devices running Fabric OS 5.2 or later.

---

To configure IP ping, complete the following steps.

1. Select **Configure > IP Troubleshooting > Ping**.  
The **IP Ping** dialog box displays.
2. Select a switch from the **Available Switches** table.
3. Select a port from the **GigE Port** list.
4. Select an IP address switch from the **IP Interface** list.
5. Enter the remote IP address in the **Remote IP Address** field.
6. Click **OK**.

Ping sends four Internet Control Message Protocol (ICMP) Ping packets to the destination address and records the time until a response.

The **IP Ping Result** dialog box displays with two tables.

The top table (**FCIP IP Ping Response Details**) contains the following statistics:

**TABLE 32** FCIP IP Ping Response Details

| Field or Component      | Description                                                                                                                                             |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status                  | Always displays 'Completed'. If there is a failure, an error message displays instead of the <b>IP Ping Result</b> dialog box.                          |
| Packets Sent            | Always displays '4'. This is not configurable.                                                                                                          |
| Packets Received        | The number of received responses.                                                                                                                       |
| Packets Lost            | Equal to the number of packets sent minus the number of packets received.                                                                               |
| Packet Lost percentage  | The number of packets lost expressed as a percentage of the packets sent. This will be 0%, 25%, 50%, 75% or 100% for 0, 1, 2, 3, or all 4 packets lost. |
| Minimum Round Trip Time | The shortest time, in milliseconds, of any response. If no response, the round trip times is 0.                                                         |
| Maximum Round Trip Time | The longest time, in milliseconds, of any response. If no response, the round trip times is 0.                                                          |
| Average Round Trip Time | The average time, in milliseconds, of all responses. If no response, the round trip times is 0.                                                         |

The bottom table (**IP Ping Details**) provides details for each ping attempt.

**TABLE 33** IP Ping Details

| Field or Component   | Description                                                                                                                                                                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reply From           | The IP address of the device that sent the reply. For a normal response, this is the destination IP address. Some error responses (such as "destination unreachable") may come from an intermediate router.                                                                                                                 |
| Status               | Displays either Success or an error message (such as request timed out or destination unreachable) from the switch.                                                                                                                                                                                                         |
| Number of bytes      | The number of bytes in the data portion of the response. Should be 64, matching the 64 bytes of data sent in the transmitted packet.                                                                                                                                                                                        |
| Round Trip Time (ms) | The time in milliseconds between sending the packet and receiving the response. This provides a rough indication of network congestion or latency. It is normal for the first packet to experience a higher round trip time than later packets, if the intermediate routers need to do ARP requests to locate the next hop. |
| Time To Live (hops)  | The number of hops remaining in the received response. The time to live is decremented by each router that forwards the packet. The packet is dropped if the time to live reaches zero.                                                                                                                                     |

7. Click **Close** on the **IP Ping Result** dialog box.
8. Click **Cancel** on the **IP Ping** dialog box.

## Tracing IP routes

The Management application enables you to select an source and a target and displays the detailed routing information from the source port or area on the local switch to the destination port or area on another switch.

Trace route cannot be performed on the offline devices or virtual devices.

---

### NOTE

Trace route is only supported on Fabric OS devices running Fabric OS 5.2 or later.

---

To trace routes, complete the following steps.

1. Select **Configure > IP Troubleshooting > Trace Route**.  
The **IP Traceroute** dialog box displays.
2. Select a switch from the **Available Switches** table.
3. Select a port from the **GigE Port** list.
4. Select an IP address switch from the **IP Interface** list.
5. Enter the remote IP address in the **Remote IP Address** field.
6. Click **OK**.

The **IP Traceroute Result** dialog box displays.

Traceroute sends three ICMP Ping packets to the destination address with a time to live (TTL) of one hop, and expects a 'TTL Expired' error back from the first router to obtain the IP address of the first hop. Traceroute then repeats the operation with a TTL of two hops to get the IP address of the second hop. This process repeats for up to ten hops, or until a successful PING response is received.

The IP Trace Details table displays the results of each attempt.

**TABLE 34** IP Trace Details

| Field or Component  | Description                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hop Number</b>   | The TTL inserted in the transmitted probe packet.                                                                                                                                 |
| <b>IP Address 1</b> | The IP address of the system that responded to the first of the three probes, or 0.0.0.0 if there was no response.                                                                |
| <b>IP Address 2</b> | The IP address of the system that responded to the second of the three probes, or 0.0.0.0 if there was no response.                                                               |
| <b>IP Address 3</b> | The IP address of the system that responded to the third of the three probes, or 0.0.0.0 if there was no response.                                                                |
| <b>RTT 1</b>        | The time in milliseconds for the first of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path.  |
| <b>RTT 2</b>        | the time in milliseconds for the second of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path. |
| <b>RTT 3</b>        | the time in milliseconds for the third of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path.  |

7. Click **Close** on the **IP Traceroute Result** dialog box.
8. Click **Cancel** on the **IP Traceroute** dialog box.

## Viewing FCIP tunnel performance

---

### NOTE

IP Performance is only supported on the 4 Gbps Router, Extension Switch and Encryption Blade running Fabric OS 5.2 or later.

---



---

### NOTE

If you run IP Performance over a link also being used for production traffic, it will impact the production traffic performance.

---

To view FCIP tunnel performance, complete the following steps.

1. Select **Configure > IP Troubleshooting > Performance**.  
The **IP Performance** dialog box displays.
2. Select a switch from the **Available Switches** table.
3. Select a port from the **GigE Port** list.
4. Select an IP address switch from the **IP Interface** list.
5. Enter the remote IP address in the **Remote IP Address** field.
6. Click **OK**.

The **IP Performance Result** dialog box displays.

IP Performance sends dummy data as fast as possible to the remote IP address and measures how much data can be sent over a given interval. IP Performance attempts to saturate the network link to see how much bandwidth is available. It will display the media link bandwidth only if no other traffic is flowing. The remote IP address must belong to a managed switch so that IP Performance can set up the receiving end on the remote switch.

For more information about IP Performance, refer to Chapter 20 in the *Fabric OS Administrator's Guide*.

During the IP Performance test, data is sent continuously and statistics are sampled every 30 seconds. At the end of the period, the IP Performance results dialog box displays. The IP Performance results dialog contains a table with one row for each 30-second sample of the test. Columns in the perf results dialog are:

| Field/Component            | Description                                                                                                                                                                                                                                                                         |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Available Bandwidth</b> | The average bytes per second sent during the sample interval. This is a count of FC payload bytes; for example, the throughput seen by an FC application. It is slightly lower than the actual bytes-per-second on the wire since it does not include headers and acknowledgements. |
| <b>Weighted Bandwidth</b>  | The weighted bandwidth represents what the FCIP tunnel / FC application sees for throughput rather than the Ethernet on-the-wire bytes.                                                                                                                                             |
| <b>Loss Percent</b>        | An estimate of the percentage of data packets lost during the sampling interval, based on TCP re-transmits.                                                                                                                                                                         |

| Field/Component                                 | Description                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DELAY</b>                                    | The average round trip time to send a packet of data and receive the acknowledgement.                                                                                                                                                                                                                                                                |
| <b>PMTU</b><br>(Path Maximum Transmission Unit) | The largest packet size that can be transmitted over the end-to-end path without fragmentation. This value is measured in bytes and includes the IP header and payload. IP Performance tries the configured Fabric OS Jumbo MTU value (anything over 15000, then 1500, then 1260. The value displayed in the table is the largest value that worked. |

7. Click **Close** on the **IP Performance Result** dialog box.
8. Click **Cancel** on the **IP Performance** dialog box.

## Client browser troubleshooting

The following section states a possible issue and the recommended solution for client browser errors.

| Problem                                                        | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Downloading Client from a Internet Explorer Browser over HTTPS | <p>If the JNLP file does not launch automatically, use one of the following options:</p> <ul style="list-style-type: none"> <li>• Complete the following steps. <ol style="list-style-type: none"> <li>1 Save the JNLP file to the local host.</li> <li>2 Launch the JNLP file manually.</li> </ol> </li> <li>• In Internet Explorer 7, complete the following steps. <ol style="list-style-type: none"> <li>1 Select <b>Tools &gt; Internet Options</b>.</li> <li>2 Click the <b>Advanced</b> tab.</li> <li>3 Clear the <b>Do not save encrypted pages to disk</b> check box.</li> </ol> </li> </ul> <p>If the browser warns you about the security certificate, use the fully qualified hostname to launch the web page.</p> |

## Fabric tracking troubleshooting

The following section states a possible issue and the recommended solution for fabric tracking errors.

| Problem                                                                                                                                                                                                                                              | Resolution                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| If a switch is replaced by another switch having the same IP address but a different node WWN while fabric tracking is on, the Management application does not update the Product List, Connectivity Map or switch properties with the new node WWN. | <p>Choose from one of the following options:</p> <ul style="list-style-type: none"> <li>• Turn fabric tracking off while the switch is replaced. This causes the old switch to be removed and the new switch added.</li> <li>• After the switch is replaced, remove and re-add the fabric in the <b>Discover Setup</b> dialog box.</li> </ul> |

## FICON troubleshooting

The following section states a possible issue and the possible cause for FICON errors.

| Problem                              | Causes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FICON not supported on switch error. | <p>FICON Unsupported Configurations:</p> <ul style="list-style-type: none"> <li>• FICON is not supported on base switches.</li> <li>• FICON is not supported on a switch which has an XISL configured.</li> <li>• FICON is not supported if the PID format is 2.</li> <li>• FICON is not supported if 10 bit address is enabled on 384-port Backbone Chassis for non-default switch.</li> <li>• FICON is not supported if any port address is greater than the maximum port number of the switch.</li> <li>• 48-port blades are not allowed in the Director Chassis for FICON.</li> <li>• FICON is not supported if virtual fabrics is disabled in the 384-port Backbone Chassis and 192-port Backbone Chassis with 48-port blades. However if virtual fabrics is enabled the 48-port blade is enabled as long as it is part of a logical switch. If the 48-port blade is part of the base switch and FMS mode is enabled, then Fabric OS persistently disables the ports.</li> <li>• FICON is not supported on Admin Domain-enabled fabrics.</li> </ul> |

## Firmware download troubleshooting

The following section states a possible issue and the recommended solution for firmware download errors.

| Problem                                                                                                                             | Resolution                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| If you configured an internal FTP server and the Management application server is running IPv6, firmware download is not supported. | <p>Choose from one of the following options:</p> <ul style="list-style-type: none"> <li>• If the Management application is running IPv6 only, configure an external FTP server.</li> <li>• If the Management application is running IPv4 and IPv6, configure IPv4 to be the preferred address.</li> </ul> |

## Launch Client troubleshooting

The following section states a possible issue and the recommended solution if you are unable to launch the client.

| Problem                                                                                                                                                                                   | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Incorrect (down level) remote client short cut displays in <b>Start</b> menu after Management application upgrade.</p> <p><b>NOTE:</b> Remote client launch requires JRE 1.6.0_16.</p> | <p>The remote client link in the <b>Start</b> menu does not automatically upgrade when you upgrade the Management application. To remove the old link and launch the correct remote client version, complete the following steps.</p> <ol style="list-style-type: none"> <li>1 Clear the previous version from the Java cache,.             <ol style="list-style-type: none"> <li>a Select <b>Start &gt; Settings &gt; Control Panel &gt; Java</b>.<br/>The <b>Java Control Panel</b> dialog box displays.</li> <li>b Click <b>View</b> on the <b>General</b> tab.<br/>The <b>Java Cache Viewer</b> dialog box displays.</li> <li>c Right-click the application and select <b>Delete</b>.</li> <li>d Click <b>Close</b> on the <b>Java Cache Viewer</b> dialog box.</li> <li>e Click <b>OK</b> on the <b>Java Control Panel</b> dialog box.</li> </ol> </li> <li>2 Log into the remote client from the browser.             <ol style="list-style-type: none"> <li>a Open a web browser and enter the IP address of the Management application server in the <b>Address</b> bar.<br/>If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, <i>IP_Address:Web_Server_Port_Number</i>.<br/>The Management application web start screen displays.</li> <li>b Click the Management application web start link.<br/>The <b>Log In</b> dialog box displays.</li> <li>c Enter your user name and password.<br/>The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.</li> <li>d Select or clear the <b>Save password</b> check box to choose whether you want the application to remember your password the next time you log in.</li> <li>e Click <b>Login</b>.</li> <li>f Click <b>OK</b> on the <b>Login Banner</b> dialog box.<br/>The Management application displays.</li> </ol> </li> </ol> |

| Problem                                                                                                                                                   | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unable to log into the Client (the application does not launch when you use a valid user name and password and exceptions are thrown in the client side). | <p>Use one the following procedures to configure the IP address in the host file.</p> <p><b>Windows operating systems</b></p> <ol style="list-style-type: none"> <li>1 Log in using the 'Administrator' privilege.</li> <li>2 Select <b>Start &gt; Run</b>.</li> <li>3 Type drivers in the <b>Open</b> field and press <b>Enter</b>.</li> <li>4 Go to the 'etc' folder and open the 'hosts' file using a text editor.</li> <li>5 Add the IP address and host name of the client in the following format: <i>IP_Address Host_Name</i>.<br/>For example, 127.0.0.1 localhost</li> <li>6 Save and exit the file.</li> </ol> <p><b>Linux/Solaris operating systems</b></p> <ol style="list-style-type: none"> <li>1 Log in using the 'root' privilege.</li> <li>2 Open the '/etc/hosts' file using a text editor.</li> <li>3 Add the IP address and host name of the client in the following format: <i>IP_Address Host_Name</i>.<br/>For example, 127.0.0.1 localhost</li> <li>4 Save and exit the file.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Unable to launch the remote client (the SSL setting, web server port number, or server starting point number changed during the server upgrade).          | <p>To remove the old link and launch the correct remote client version, complete the following steps.</p> <ol style="list-style-type: none"> <li>1 Clear the previous version from the Java cache,.             <ol style="list-style-type: none"> <li>a Select <b>Start &gt; Settings &gt; Control Panel &gt; Java</b>.<br/>The <b>Java Control Panel</b> dialog box displays.</li> <li>b Click <b>View</b> on the <b>General</b> tab.<br/>The <b>Java Cache Viewer</b> dialog box displays.</li> <li>c Right-click the application and select <b>Delete</b>.</li> <li>d Click <b>Close</b> on the <b>Java Cache Viewer</b> dialog box.</li> <li>e Click <b>OK</b> on the <b>Java Control Panel</b> dialog box.</li> </ol> </li> <li>2 Log into the remote client from the browser.             <ol style="list-style-type: none"> <li>a Open a web browser and enter the IP address of the Management application server in the <b>Address</b> bar.<br/>If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, <i>IP_Address:Web_Server_Port_Number</i>.<br/>The Management application web start screen displays.</li> <li>b Click the Management application web start link.<br/>The <b>Log In</b> dialog box displays.</li> <li>c Enter your user name and password.<br/>The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.</li> <li>d Select or clear the <b>Save password</b> check box to choose whether you want the application to remember your password the next time you log in.</li> <li>e Click <b>Login</b>.</li> <li>f Click <b>OK</b> on the <b>Login Banner</b> dialog box.<br/>The Management application displays.</li> </ol> </li> </ol> |

## Names troubleshooting

The following section states a possible issue and the recommended solution for names errors.

| Problem               | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Duplicate name error. | <p>If you configured the Management application to only allow unique names and you try to use a name that already exists in the fabric. You can enter a different name for the device or search for the duplicate name using one of the following procedures:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Searching for a device by name”</a> on page 82 in the <b>Configure Names</b> dialog box</li> <li>• <a href="#">“Searching for a device by WWN”</a> on page 83 in the <b>Configure Names</b> dialog box</li> <li>• <a href="#">“Searching for a device in the connectivity map”</a> on page 139</li> </ul> |

## Performance troubleshooting

The following section states a possible issue and the recommended solution for Performance errors.

| Problem                                                                                                                                          | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>An error message with the following text displays:<br/>Real Time statistics collection has failed.<br/>Please see master log for details.</p> | <p>Make sure that the following prerequisites for Performance Monitoring Data collection are met.</p> <ol style="list-style-type: none"> <li>1 To collect performance statistics for any protocol type (FC/FCIP/FCOE/GE), the snmp access control list must have an empty list or the Management server IP must be included in the access control list.<br/>For example, data collection occurs in the following cases.<br/>Case 1: Default access control list is empty<br/> <pre>FCRRouter:admin&gt; snmpconfig --show accesscontrol</pre> <p>SNMP access list configuration:</p> <pre>Entry 0: No access host configured yet Entry 1: No access host configured yet Entry 2: No access host configured yet Entry 3: No access host configured yet Entry 4: No access host configured yet Entry 5: No access host configured yet</pre> <br/> Case 2: Management Server IP included in access control list<br/> <pre>FCRRouter:admin&gt; snmpconfig --show accesscontrol</pre> <p>SNMP access list configuration:</p> <pre>Entry 0: Access host subnet area 172.26.1.86 (rw) Entry 1: No access host configured yet Entry 2: No access host configured yet Entry 3: No access host configured yet Entry 4: No access host configured yet Entry 5: No access host configured yet</pre> <p><b>Verification and Troubleshooting.</b><br/>To add the server IP address to the access control list, use the following command from the switch CLI:<br/> <pre>FCRRouter:admin&gt; snmpconfig --set accesscontrol</pre><br/> To set the default access control, use the following command from the switch CLI:<br/> <pre>FCRRouter:admin&gt; snmpconfig --default accesscontrol</pre></p> </li> </ol> |

| Problem                                                                                                                                 | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| An error message with the following text displays:<br>Real Time statistics collection has failed.<br>Please see master log for details. | <p>2 To collect data, the SNMP credentials in the Management application and switch must match.</p> <p>SNMP v1 or v3: The community strings entered in the <b>Address Properties</b> dialog box - <b>SNMP</b> tab must match the one entered in the switch.</p> <p>If you enter 'test' as the SNMP v1 community string in the Management application, then the community string in the switch must be 'test' as well.</p> <p>To view the switch SNMP value, use one of the following commands from the switch CLI:</p> <pre>HCLSwitch:admin&gt; snmpconfig --show snmpv1 HCLSwitch:admin&gt; snmpconfig --show snmpv3</pre> <p>To set the switch SNMP value, use one of the following commands from the switch CLI:</p> <pre>HCLSwitch:admin&gt; snmpconfig --set snmpv1 HCLSwitch:admin&gt; snmpconfig --set snmpv3</pre> <p><b>Example</b></p> <pre>HCLSwitch:admin&gt; snmpconfig --set snmpv1 SNMP community and trap recipient configuration: Community (rw): [test] Trap Recipient's IP address : [172.26.1.183] Trap recipient Severity level : (0..5) [4] Trap recipient Port : (0..65535) [162] Community (rw): [OrigEquipMfr] Trap Recipient's IP address : [172.26.24.26] Trap recipient Severity level : (0..5) [4] Trap recipient Port : (0..65535) [162] Community (rw): [custom] Trap Recipient's IP address : [172.26.1.158] Trap recipient Severity level : (0..5) [4] Trap recipient Port : (0..65535) [162] Community (ro): [custom] Trap Recipient's IP address : [0.0.0.0] Community (ro): [common] Trap Recipient's IP address : [0.0.0.0] Community (ro): [FibreChannel] Trap Recipient's IP address : [172.26.1.145] Trap recipient Severity level : (0..5) [4] Trap recipient Port : (0..65535) [162]</pre> |

| Problem                                                                                                                                 | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| An error message with the following text displays:<br>Real Time statistics collection has failed.<br>Please see master log for details. | <p>3 To collect GigE port and FCIP statistics, you must enable the FCIP-MIB capability.</p> <p><b>Verification and Troubleshooting</b></p> <p>To verify that FCIP-MIB capability is enabled, use the following command from the switch CLI:</p> <pre>FCRRouter:admin&gt; snmpconfig --show mibcapability FCIP-MIB: YES</pre> <p>To enabling FCIP-MIB capability, use the following command from the switch CLI:</p> <pre>FCRRouter:admin&gt; snmpconfig --set mibcapability FA-MIB (yes, y, no, n): [yes] FICON-MIB (yes, y, no, n): [yes] HA-MIB (yes, y, no, n): [yes] FCIP-MIB (yes, y, no, n): [yes] ISCSI-MIB (yes, y, no, n): [yes]</pre> <p>4 To collect FCIP or GE statistics, you must configure SNMPv3 credentials in the <b>Address Properties</b> dialog box - <b>SNMP</b> tab.</p> <p>Verify that the SNMPv3 credentials are valid. When you discover a switch using 'admin' as the v3 credentials, a new user (for example, User 6) is created with the SNMP user name 'admin'. To verify the SNMP user credentials, use the following command from the switch CLI:</p> <pre>sw1:FID128:admin&gt; snmpconfig --show snmpv3</pre> <p>SNMPv3 USM configuration:</p> <pre>User 1 (rw): snmpadmin1 Auth Protocol: noAuth Priv Protocol: noPriv User 2 (rw): snmpadmin2 Auth Protocol: noAuth Priv Protocol: noPriv User 3 (rw): snmpadmin3 Auth Protocol: noAuth Priv Protocol: noPriv User 4 (ro): snmpuser1 Auth Protocol: noAuth Priv Protocol: noPriv User 5 (ro): snmpuser2 Auth Protocol: noAuth Priv Protocol: noPriv User 6 (ro): admin Auth Protocol: noAuth Priv Protocol: noPriv</pre> |

| Problem                                                                                                                                 | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| An error message with the following text displays:<br>Real Time statistics collection has failed.<br>Please see master log for details. | <p>5 To collect data on Virtual Fabric-enabled switches, the Fabric OS user must have access to all Virtual Fabrics. The SNMPv3 user name must be the same as the Fabric OS user name. If the SNMPv3 and Fabric OS user names do not match, data is not collected for the virtual switches with the non-default VF ID. By default, the user 'admin' has access to all Virtual Fabrics.</p> <p>To verify the Fabric OS user (verify Role-LF List), use the following command from the switch CLI:</p> <pre>swl:FID128:admin&gt; userconfig --show</pre> <pre>Account name: admin Description: Administrator Enabled: Yes Password Last Change Date: Unknown Password Expiration Date: Not Applicable Locked: No Home LF Role: admin Role-LF List: admin: 1-128 Chassis Role: admin Home LF: 128</pre>                                                                                                                                        |
|                                                                                                                                         | <p>6 To collect real time data, I/O must be running in the switch. To view the statistics in the switch, use one of the following command:</p> <p>FC Ports command from the switch CLI:</p> <pre>portperfshow &lt;interval&gt;</pre> <p><b>Example</b> Sprint-65:root&gt; portperfshow 5</p> <p>FCIP tunnels: command:</p> <pre>portshow fciptunnel &lt;Ge port number&gt; &lt;tunnel no&gt; -perf</pre> <p><b>Example</b> Sprint-65:root&gt; portshow fciptunnel ge0 1 -perf</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| An error message with the following text displays:<br>Real Time statistics collection has failed.<br>Please see master log for details. | <p>7 To collect performance statistics from a switch, the SNMP security level must be set correctly in the switch. For example, a secLevel of '3' means "No access" which stops the management application from collecting performance statistics from the switch. To show the security level respectively, use the following command from the switch CLI:</p> <pre>snmpconfig --show secLevel</pre> <p><b>Example</b></p> <pre>snmpconfig --show secLevel</pre> <pre>GET security level = 0, SET level = 0 SNMP GET Security Level: No security SNMP SET Security Level: No security</pre> <p>To set the security level respectively, use the following command from the switch CLI:</p> <pre>snmpconfig --set secLevel</pre> <p><b>Example</b></p> <pre>snmpconfig --set secLevel 0</pre> <pre>Select SNMP GET Security Level (0 = No security, 1 = Authentication only, 2 = Authentication and Privacy, 3 = No Access): (0..3) [0]</pre> |

## Port Fencing troubleshooting

The following section states a possible issue and the recommended solution for Port Fencing errors.

| Problem                                                                                                                                                                                                                                                                                                                                                     | Resolution                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| In a pure M-EOS fabric, fabric level policy information (for example, Port Fencing Link threshold) is stored in database based on the principle switch WWN. Therefore, if you add a switch to the fabric and the new switch becomes the Principle switch, the Management application cannot obtain the policy information and the threshold is not applied. | Re-assign the threshold to the fabric. For step-by-step instructions, refer to <a href="#">“Assigning thresholds”</a> on page 339. |
| If you segment a switch from a fabric then rediscover the switch without accepting changes, the <b>Port Fencing</b> dialog box displays the switch twice and the port count is doubled.                                                                                                                                                                     | Right-click on the fabric that the segmented switch (with red minus icon) is part of and select <b>Accept Changes</b> .            |

## Server Management Console troubleshooting

The following section states a possible issue and the recommended solution for server management console.

| Problem                                                         | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unable to launch the SMC on a Windows Vista or Windows 7 system | <p>The Windows Vista or Windows 7 system enables the User Access Control (UAC) option by default. When the UAC option is enabled, the SMC cannot launch. If the SMC does not launch, use one of the following options to disable the UAC option:</p> <p>The following are the various ways we can disable UAC in vista:</p> <p><b>Disable using msconfig by completing the following steps.</b></p> <ol style="list-style-type: none"> <li>1 Select <b>Start &gt; Run</b>.</li> <li>2 Type msconfig on the <b>Run</b> dialog box and click <b>OK</b>.</li> <li>3 Click the <b>Tools</b> tab on the <b>System Configuration Utility</b>.</li> <li>4 Scroll down to and select the <b>Disable UAC</b> tool name.</li> <li>5 Click <b>Launch</b>.</li> </ol> <p>A command window displays and runs the disable UAC command. When the command is complete, close the window.</p> <ol style="list-style-type: none"> <li>6 Close the <b>System Configuration Utility</b>.</li> <li>7 Restart the computer to apply changes.</li> </ol> <p><b>NOTE:</b> You can re-enable UAC using the above procedure and selecting the <b>Enable UAC</b> tool name in step 4.</p> <p><b>Disable using regedit by completing the following steps.</b></p> <p><b>NOTE:</b> Before making changes to the registry, make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes.</p> <ol style="list-style-type: none"> <li>1 Select <b>Start &gt; Run</b>.</li> <li>2 Type regedit on the <b>Run</b> dialog box and click <b>OK</b>.</li> <li>3 Navigate to the following registry key:<br/>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System</li> <li>4 Right-click the <b>EnableLUA</b> value and select <b>Modify</b>.</li> <li>5 Change the <b>Value data</b> field to 0 on the <b>Edit DWORD Value</b> dialog box and click <b>OK</b>.</li> <li>6 Close the <b>Registry Editor</b>.</li> <li>7 Restart the computer to apply changes.</li> </ol> <p><b>NOTE:</b> You can re-enable UAC using the above procedure and changing the <b>Value data</b> field to 1 in step 5.</p> |

| Problem                                                                      | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unable to launch the SMC on a Windows Vista or Windows 7 system<br>continued | <p><b>Disable using the Group Policy by completing the following steps.</b></p> <p>You can perform this procedure on you local machine using Local Group Policy editor or for many computers at the same time using the Active Directory-based Group Policy Object (GPO) editor.</p> <p>To disable using the Local Group Policy editor, complete the following steps.</p> <ol style="list-style-type: none"> <li>1 On your local Vista computer, select <b>Start &gt; Run</b>.</li> <li>2 Type gpedit.msc on the <b>Run</b> dialog box and click <b>OK</b>.</li> <li>3 Browse to <b>Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Local Policies &gt; Security Options</b> in the Group Policy editor.</li> <li>4 In the right pane scroll to the User Access Control policies (at the bottom of the pane).</li> <li>5 Right-click the <b>Behavior of the elevation prompt for Administrators in Admin Approval Mode</b> policy and select <b>Properties</b>.</li> <li>6 Select the <b>No Prompt</b> option and click <b>OK</b>.</li> <li>7 Right-click the <b>Detect application installations and prompt for elevation</b> policy and select <b>Properties</b>.</li> <li>8 Select the <b>Disabled</b> option and click <b>OK</b>.</li> <li>9 Right-click the <b>Run all administrators in Admin Approval Mode</b> policy and select <b>Properties</b>.</li> <li>10 Select the <b>Disabled</b> option and click <b>OK</b>.</li> <li>11 Close the Group Policy editor.</li> <li>12 Restart the computer to apply changes.</li> </ol> <p>To disable using the Active Directory-based GPO editor, complete the following steps.</p> <ol style="list-style-type: none"> <li>1 On a Vista computer that is a member of a domain, select <b>Start &gt; Run</b>.</li> <li>2 Type gpedit.msc on the <b>Run</b> dialog box and click <b>OK</b>.</li> <li>3 Browse to the required GPO that is linked to the OU or domain where the Vista computers are located, then edit it</li> <li>4 Browse to <b>Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Local Policies &gt; Security Options</b> in the Group Policy editor.</li> <li>5 In the right pane scroll to the User Access Control policies (at the bottom of the pane).</li> <li>6 Right-click the <b>Behavior of the elevation prompt for Administrators in Admin Approval Mode</b> policy and select <b>Properties</b>.</li> <li>7 Select the <b>No Prompt</b> option and click <b>OK</b>.</li> <li>8 Right-click the <b>Detect application installations and prompt for elevation</b> policy and select <b>Properties</b>.</li> <li>9 Select the <b>Disabled</b> option and click <b>OK</b>.</li> <li>10 Right-click the <b>Run all administrators in Admin Approval Mode</b> policy and select <b>Properties</b>.</li> <li>11 Select the <b>Disabled</b> option and click <b>OK</b>.</li> <li>12 Close the Group Policy editor.</li> <li>13 Restart the computer to apply changes.</li> </ol> |

## Supportsave troubleshooting

The following section states a possible issue and the recommended solution for supportsave errors.

| Problem                                  | Resolution                                                                                                                                                                                                                                                                                                             |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot capture support save information. | <p>Capture support show by running the batch file from the <i>Install_Home/bin/supportshow.bat</i> from Windows and UNIX systems.</p> <ol style="list-style-type: none"> <li>1 Open <i>Install_Home\bin\supportsave.bat</i>.</li> <li>2 Edit file supportsave dbuser dbpasswd [tareget-dir] [pause-option].</li> </ol> |

## View All list troubleshooting

The following section states a possible issue and the recommended solution for **View All** list errors.

| Problem                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Resolution                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View All</b> list does not display.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | The <b>View All</b> list does not display until you discover a fabric. To discover a fabric, refer to <a href="#">“Discovering fabrics”</a> on page 36. |
| <b>View All</b> list does not display and there are discovered fabrics.<br><b>Example</b><br>If you create a new view 'V1' that has one fabric 'F1' and you display the new view in the SAN tab (select <b>V1</b> from the <b>View All</b> list). Then you delete the fabric F1 from Discovery, the <b>View All</b> list no longer displays and the following messages displays:<br>View loaded, no devices present in the current view. Refer to the Troubleshooting Guide in Help (F1) for assistance. | To select another view, select <b>View &gt; Manage View &gt; Display View &gt; View_Name</b> .                                                          |

## Zoning troubleshooting

The following section states some possible issues and recommended solutions for zoning errors.

| Problem                                                                                                                                                                                                  | Resolution                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot perform zoning on a new switch.                                                                                                                                                                   | You must use telnet (or the <b>Product Type and Access</b> tab in the <b>Add Properties</b> dialog box) to change the default password on the new switch before you can use the Management application to perform zoning. |
| When configuring a large zone configuration a switch displays offline during discovery.                                                                                                                  | If a large zone configuration is configured in a fabric, switches may temporarily display as being offline during discovery.<br>Wait for the next discovery cycle and click the <b>Refresh</b> button on the toolbar.     |
| When activating a large zone configuration on a two-switch fabric on UNIX platforms, an error message displays stating “Failed to perform the requested zoning action: Failed to zone due to exception.” | Although the error message states that the requested zoning action failed, the zone configuration will be correctly activated. Wait for the next zoning polling to occur.<br>This issue only occurs on UNIX systems.      |
| Zoning activation message displays for a long time, but zone configuration is not activated.                                                                                                             | Telnet zoning can take a long time. To improve speed, open the <b>Discover Setup</b> dialog box ( <b>Discover &gt; Setup</b> ) and add the IP address for the device to the <b>Selected Individual Addresses</b> list.    |
| Out of memory error caused by running a zoning report for a large zone configuration (1 MB) in a medium-sized SAN due to a third party tool.                                                             | You must increase the client memory allocation by completing <a href="#">“Configuring memory allocation settings”</a> on page 97.                                                                                         |

# Application menus

## In this appendix

- [Main menus . . . . .](#) 675
- [Shortcut menus . . . . .](#) 682

## Main menus

The menu bar is located at the top of the main window. The following table outlines the many functions available on each menu.

| Menu        | Command                                                                                   | Command Options                                                    |
|-------------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Server Menu |                                                                                           |                                                                    |
|             | <b>Users.</b> Select to configure users and user groups.                                  |                                                                    |
|             | <b>Active Sessions.</b> Select to display the active Management application sessions.     |                                                                    |
|             | <b>Server Properties.</b> Select to display the Server properties.                        |                                                                    |
|             | <b>Options.</b> Select to configure the Management application options.                   |                                                                    |
|             | <b>Exit.</b> Select to close the Management Client.                                       |                                                                    |
| Edit Menu   |                                                                                           |                                                                    |
|             | <b>Copy.</b> Select to copy information and move it to another location.                  |                                                                    |
|             | <b>Show Connections.</b> Select to show connections in a group.                           |                                                                    |
|             | <b>Select All.</b> Select to select all objects in the Connectivity Map and Product List. |                                                                    |
|             | <b>Properties.</b> Select to display the selected objects properties.                     |                                                                    |
| View Menu   |                                                                                           |                                                                    |
|             | <b>Show Panels.</b> Select to select which panels to display.                             |                                                                    |
|             |                                                                                           | <b>All Panels.</b> Select to show all panels.                      |
|             |                                                                                           | <b>Connectivity Map.</b> Select to only show the connectivity map. |
|             |                                                                                           | <b>Product List.</b> Select to only show the Product List.         |
|             |                                                                                           | <b>Master Log.</b> Select to only show the Master Log.             |

## A Main menus

| Menu | Command                                                                                                            | Command Options                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
|      | <b>Manage View.</b> Select to set up the Management application view.                                              |                                                                                                  |
|      |                                                                                                                    | <b>Create View.</b> Select to create a new view.                                                 |
|      |                                                                                                                    | <b>Display View.</b> Select to display by View All or by a view you create.                      |
|      |                                                                                                                    | <b>Levels.</b> Select to display by All Levels, Products and Ports, Product Only, or Ports Only. |
|      |                                                                                                                    | <b>Copy View.</b> Select to copy a view.                                                         |
|      |                                                                                                                    | <b>Delete View.</b> Select to delete a view.                                                     |
|      |                                                                                                                    | <b>Edit View.</b> Select to edit a view.                                                         |
|      | <b>Zoom.</b> Select to configure the zoom percentage.                                                              |                                                                                                  |
|      | <b>Show.</b> Select to determine what products display.                                                            |                                                                                                  |
|      |                                                                                                                    | <b>Fabrics Only.</b> Select to display only fabrics.                                             |
|      |                                                                                                                    | <b>Groups Only.</b> Select to display only groups.                                               |
|      |                                                                                                                    | <b>All Products.</b> Select to display all products.                                             |
|      |                                                                                                                    | <b>All Ports.</b> Select to display all ports.                                                   |
|      | <b>Enable Flyover Display/Device Tips.</b> Select to enable flyover display.                                       |                                                                                                  |
|      | <b>Show Ports.</b> Select to show utilized ports on the selected device.                                           |                                                                                                  |
|      | <b>Connected End Devices.</b> Select to show or hide all connected end devices.                                    |                                                                                                  |
|      |                                                                                                                    | <b>Include Virtual Devices</b> check box. Select to include virtual devices.                     |
|      |                                                                                                                    | <b>Hide All.</b> Select to hide all connected end devices.                                       |
|      |                                                                                                                    | <b>Show All.</b> Select to show all connected end devices.                                       |
|      |                                                                                                                    | <b>Custom.</b> Select to set a custom display for all connected end devices.                     |
|      |                                                                                                                    | <i>MyCustomList.</i> Lists all custom views.                                                     |
|      | <b>Map Display.</b> Select to customize a group's layout to make it easier to view the SAN and manage its devices. |                                                                                                  |
|      | <b>Domain ID/Port #.</b> Select to set the display domain IDs and port numbers in decimal or hex format.           |                                                                                                  |
|      |                                                                                                                    | <b>Decimal.</b> Select to display all domain IDs and port numbers in decimal format.             |
|      |                                                                                                                    | <b>Hex.</b> Select to display all domain IDs in hex format.                                      |

| Menu                 | Command                                                                                                       | Command Options                                                                                                                                                 |
|----------------------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <b>Product Label.</b> Select to configure which product labels display.                                       |                                                                                                                                                                 |
|                      |                                                                                                               | <b>Name.</b> Select to display the product name as the product label.                                                                                           |
|                      |                                                                                                               | <b>Node WWN.</b> Select to display the node name as the product label.                                                                                          |
|                      |                                                                                                               | <b>IP Address.</b> Select to display the IP Address (IPv4 or IPv6 format) as the product label.                                                                 |
|                      |                                                                                                               | <b>Domain ID.</b> Select to display the domain ID as the product label.                                                                                         |
|                      | <b>Port Label.</b> Select to configure which port labels display.                                             |                                                                                                                                                                 |
|                      |                                                                                                               | <b>Name.</b> Select to display the name as the port label.                                                                                                      |
|                      |                                                                                                               | <b>Port #.</b> Select to display the port number as the port label.                                                                                             |
|                      |                                                                                                               | <b>Port Address.</b> Select to display the port address as the port label.                                                                                      |
|                      |                                                                                                               | <b>Port WWN.</b> Select to display the port world wide name as the port label.                                                                                  |
|                      |                                                                                                               | <b>User Port #.</b> Select to display the user port number as the port label.                                                                                   |
|                      |                                                                                                               | <b>Slot/Port #.</b> Select to display the slot/port number as the port label.                                                                                   |
|                      | <b>Port Display.</b> Select to configure how ports display.                                                   |                                                                                                                                                                 |
|                      |                                                                                                               | <b>Occupied Product Ports.</b> Select to display the ports of the devices in the fabrics (present in the Connectivity Map) that are connected to other devices. |
|                      |                                                                                                               | <b>UnOccupied Product Ports.</b> Select to display the ports of the devices (shown in the Connectivity Map) that are not connected to any other device.         |
|                      |                                                                                                               | <b>Attached Ports.</b> Select to display the attached ports of the target devices.                                                                              |
|                      |                                                                                                               | <b>Switch to Switch Connections.</b> Select to display the switch-to-switch connections.                                                                        |
| <b>Discover Menu</b> |                                                                                                               |                                                                                                                                                                 |
|                      | <b>Setup.</b> Select to set up Discovery.                                                                     |                                                                                                                                                                 |
|                      | <b>Server Port Mapping.</b> Select to manually map ports to a server.                                         |                                                                                                                                                                 |
|                      | <b>Storage Port Mapping.</b> Select to manually map Storage Ports to a Storage Device or other Storage Ports. |                                                                                                                                                                 |

## A Main menus

| Menu                  | Command                                                                     | Command Options                                                                                                                                                              |
|-----------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configure Menu</b> |                                                                             |                                                                                                                                                                              |
|                       | <b>Element Manager.</b> Select to configure a selected device.              |                                                                                                                                                                              |
|                       |                                                                             | <b>Hardware.</b> Select to the Element Manager or Web Tools application for the selected device.                                                                             |
|                       |                                                                             | <b>Ports.</b> Select to launch Web Tools for the selected device.                                                                                                            |
|                       |                                                                             | <b>Admin.</b> Select to launch Web Tools for the selected device.                                                                                                            |
|                       |                                                                             | <b>Router Admin.</b> Select to launch Web Tools for the selected device.                                                                                                     |
|                       | <b>Switch.</b> Select to manage a selected device.                          |                                                                                                                                                                              |
|                       |                                                                             | <b>Save.</b> Select to save device configurations to the repository.                                                                                                         |
|                       |                                                                             | <b>Save Running to Startup.</b> Select to save the CEE running configuration to the startup configuration on selected switches. Requires at least one discovered CEE switch. |
|                       |                                                                             | <b>Restore.</b> Select to restore device configurations from the repository.                                                                                                 |
|                       |                                                                             | <b>CEE.</b> Select to manage a CEE switch, port, or link aggregation group (LAG).                                                                                            |
|                       |                                                                             | <b>FCoE.</b> Select to manage an FCoE port.                                                                                                                                  |
|                       |                                                                             | <b>Configuration Repository.</b> Select to manage device configurations from the repository.                                                                                 |
|                       |                                                                             | <b>Schedule Backup.</b> Select to schedule configuration backup.                                                                                                             |
|                       |                                                                             | <b>Replicate.</b> Select to replicate the switch Configuration or Security.                                                                                                  |
|                       |                                                                             | <b>Swap Blades.</b> Select to swap blades.                                                                                                                                   |
|                       | <b>Firmware Management.</b> Select to download firmware to devices.         |                                                                                                                                                                              |
|                       | <b>Routing.</b> Select to manage a selected router.                         |                                                                                                                                                                              |
|                       |                                                                             | <b>Configuration.</b> Select to view the R_Ports on a router.                                                                                                                |
|                       |                                                                             | <b>Domain IDs.</b> Select to configure the router domain IDs.                                                                                                                |
|                       | <b>Logical Switches.</b> Select to configure logical switches for your SAN. |                                                                                                                                                                              |
|                       | <b>Encryption.</b> Select to configure encryption for your SAN.             |                                                                                                                                                                              |
|                       | <b>Zoning.</b> Select to configure zones.                                   |                                                                                                                                                                              |
|                       |                                                                             | <b>Fabric.</b> Select to configure fabric zones.                                                                                                                             |
|                       |                                                                             | <b>LSAN.</b> Select to configure LSAN zones.                                                                                                                                 |
|                       |                                                                             | <b>Set Change Limits.</b> Select to set zone limits for zone activation.                                                                                                     |

| Menu | Command                                                                                                                                                                                                                                                                                                                                                                                               | Command Options                                                                                                                          |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
|      | <b>Names.</b> Select to provide familiar simple names to products and ports in your SAN.                                                                                                                                                                                                                                                                                                              |                                                                                                                                          |
|      | <b>FCIP Tunnels.</b> Select to connect to remote fabrics.                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                          |
|      | <b>High Integrity Fabric.</b> Select to activate the following on M-EOS and Fabric OS devices: <ul style="list-style-type: none"> <li>On M-EOS switches, HIF activates fabric binding, switch binding, insistent domain ID and RSCNs.</li> <li>On Fabric OS switches, HIF activates SCC policy, sets Insistent Domain ID and sets Fabric Wide Consistency Policy for SCC in tolerant mode.</li> </ul> |                                                                                                                                          |
|      | <b>Fabric Binding.</b> Select to configure whether switches can merge with a selected fabric, which provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.                                                                                                                                                          |                                                                                                                                          |
|      | <b>Port Fencing.</b> Select to configure port fencing to protect your SAN from repeated operational or security problems experienced by ports.                                                                                                                                                                                                                                                        |                                                                                                                                          |
|      | <b>Port Auto Disable.</b> Select to configure port auto disable flag on individual FC_ports or all ports on a selected device, as well as unblock currently blocked ports.                                                                                                                                                                                                                            |                                                                                                                                          |
|      | <b>FICON.</b> Select to configure FICON.                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                          |
|      |                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Configure Fabric.</b> Select to configure cascaded FICON from the selected fabric.                                                    |
|      |                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Merge Fabrics.</b> Select to merge the selected fabrics.                                                                              |
|      | <b>Allow/Prohibit Matrix.</b> Select to allow FICON users to configure an Allow/Prohibit Matrix table. You can select any matrix tables and compare them either vertically or horizontally.                                                                                                                                                                                                           |                                                                                                                                          |
|      | <b>Port Groups.</b> Select to configure a group of ports from one or more switches within the same fabric.                                                                                                                                                                                                                                                                                            |                                                                                                                                          |
|      | <b>FC Troubleshooting.</b> Select to troubleshoot your SAN.                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                          |
|      |                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Trace Route.</b> Select to view the route information between two device ports.                                                       |
|      |                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Device Connectivity.</b> Select to view the connectivity information for two devices.                                                 |
|      |                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Fabric Device Sharing.</b> Select to determine if the selected fabrics are configured to share devices.                               |
|      | <b>IP Troubleshooting.</b> Select to troubleshoot your IP.                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                          |
|      |                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Ping.</b> Select to perform a zoning check between the selected device port WWNs.                                                     |
|      |                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Trace Route.</b> Select to view the route information from a source port on the local device to a destination port on another device. |
|      |                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Performance.</b> Select to view IP performance between two devices.                                                                   |

## A Main menus

| Menu                 | Command                                                                                                                            | Command Options                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <b>List Zone Members.</b> Select to display all members in a zone.                                                                 |                                                                                                                                                                                                                                          |
| <b>Monitor Menu.</b> |                                                                                                                                    |                                                                                                                                                                                                                                          |
|                      | <b>Performance.</b> Select to monitor SAN devices.                                                                                 |                                                                                                                                                                                                                                          |
|                      |                                                                                                                                    | <b>View Utilization.</b> Select to display connection utilization.                                                                                                                                                                       |
|                      |                                                                                                                                    | <b>Historical Data Collection.</b> Select how to monitor historical data by choosing one of the following options: <ul style="list-style-type: none"> <li>• Enable SAN Wide</li> <li>• Enable Selected</li> <li>• Disable All</li> </ul> |
|                      |                                                                                                                                    | <b>End-to-End Monitors.</b> Select to monitor end-to-end connections.                                                                                                                                                                    |
|                      |                                                                                                                                    | <b>Configure Thresholds.</b> Select to monitor thresholds.                                                                                                                                                                               |
|                      |                                                                                                                                    | <b>Clear Counters.</b> Select to clear all port statistics counters.                                                                                                                                                                     |
|                      |                                                                                                                                    | <b>Top Talkers.</b> Select to monitor performance through a real-time list of top conversations for a switch or port along with related information.                                                                                     |
|                      |                                                                                                                                    | <b>Real-Time Graph.</b> Select to monitor performance through a graph, which displays transmit and receive data. The graphs show real-time data.                                                                                         |
|                      |                                                                                                                                    | <b>Historical Graph.</b> Select to monitor a performance through a graph, which displays transmit and receive data. The graphs show historical data.                                                                                     |
|                      |                                                                                                                                    | <b>Historical Report.</b> Select to monitor a performance through a table, which displays transmit and receive data. The table shows historical data.                                                                                    |
|                      | <b>Technical Support.</b> Select to configure technical support data.                                                              |                                                                                                                                                                                                                                          |
|                      |                                                                                                                                    | <b>Client SupportSave.</b> Select to capture client support data.                                                                                                                                                                        |
|                      |                                                                                                                                    | <b>Switch/Host SupportSave.</b> (Fabric OS devices only) Select to configure technical support data collection.                                                                                                                          |
|                      |                                                                                                                                    | <b>Upload Failure Data Capture.</b> Select to configure capture failure data for Fabric OS devices.                                                                                                                                      |
|                      |                                                                                                                                    | <b>View Repository.</b> Select to view repository data.                                                                                                                                                                                  |
|                      | <b>Event Policies.</b> Select to configure event policies.                                                                         |                                                                                                                                                                                                                                          |
|                      | <b>Event Notification.</b> Select to configure the Management application to send event notifications at specified time intervals. |                                                                                                                                                                                                                                          |
|                      |                                                                                                                                    | <b>E-mail.</b> Select to configure the Management application to send event notifications through e-mail.                                                                                                                                |
|                      |                                                                                                                                    | <b>Call Home.</b> Select to configure the Management Server to automatically dial-in to or send an E-mail to a support center to report system problems.                                                                                 |
|                      | <b>SNMP Setup.</b> Select to configure SNMP traps.                                                                                 |                                                                                                                                                                                                                                          |

| Menu                | Command                                                                                                                                                                                                                                                                                         | Command Options                                                                                                    |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
|                     | <b>Syslog Configuration.</b> Select to configure Syslog for the management server.                                                                                                                                                                                                              |                                                                                                                    |
|                     | <b>Logs.</b> Select to display logs.                                                                                                                                                                                                                                                            |                                                                                                                    |
|                     |                                                                                                                                                                                                                                                                                                 | <b>Audit.</b> Select to display a history of user actions performed through the application (except login/logout). |
|                     |                                                                                                                                                                                                                                                                                                 | <b>Event.</b> Select to display errors related to SNMP traps and Client-Server communications.                     |
|                     |                                                                                                                                                                                                                                                                                                 | <b>Fabric.</b> Select to display the events related to the selected fabric.                                        |
|                     |                                                                                                                                                                                                                                                                                                 | <b>FICON.</b> Select to display the FICON events related to the selected device or fabric.                         |
|                     |                                                                                                                                                                                                                                                                                                 | <b>Product Status.</b> Select to display operational status changes of managed products.                           |
|                     |                                                                                                                                                                                                                                                                                                 | <b>Security.</b> Select to display security information.                                                           |
|                     |                                                                                                                                                                                                                                                                                                 | <b>Syslog.</b> Select to display Syslog events related to the selected device or fabric.                           |
|                     | <b>Track Fabric Changes.</b> Select to track fabric changes on the selected fabric.                                                                                                                                                                                                             |                                                                                                                    |
|                     | <b>Accept Change(s).</b> Select to accept changes to the selected fabric.                                                                                                                                                                                                                       |                                                                                                                    |
|                     | <b>Port Connectivity.</b> Select to view port connectivity on the selected device.                                                                                                                                                                                                              |                                                                                                                    |
|                     | <b>Port Optics (SFP).</b> Select to display the properties associated with a selected small form-factor pluggable (SFP) transceiver on the selected device.                                                                                                                                     |                                                                                                                    |
|                     | <b>Events.</b> Select to display all events triggered on the selected device.                                                                                                                                                                                                                   |                                                                                                                    |
| <b>Reports Menu</b> |                                                                                                                                                                                                                                                                                                 |                                                                                                                    |
|                     | <b>Generate.</b> Select to determine which reports to run.                                                                                                                                                                                                                                      |                                                                                                                    |
|                     | <b>View.</b> Select to view reports through the application or through an internet browser.                                                                                                                                                                                                     |                                                                                                                    |
| <b>Tools Menu</b>   |                                                                                                                                                                                                                                                                                                 |                                                                                                                    |
|                     | <b>Setup.</b> Select to set up the applications that display on the <b>Tools</b> menu.                                                                                                                                                                                                          |                                                                                                                    |
|                     | <b>Product Menu.</b> Select to access the tools available on a device's shortcut menu.                                                                                                                                                                                                          |                                                                                                                    |
|                     | <b>Plug-in for VMware vCenter.</b> Select to configure VMWare vCenters.                                                                                                                                                                                                                         |                                                                                                                    |
|                     | <b>Tools List (determined by user settings).</b> Select to open a software application. You can configure the <b>Tools</b> menu to display different software applications. Recommended tools to include in this menu include an internet browser, the command prompt application, and Notepad. |                                                                                                                    |

## A Shortcut menus

| Menu             | Command                                                                                                                                          | Command Options |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Help Menu</b> |                                                                                                                                                  |                 |
|                  | <b>Contents.</b> Select to open the Online Help.                                                                                                 |                 |
|                  | <b>Find.</b> Select to search the Online Help.                                                                                                   |                 |
|                  | <b>License.</b> Select to view or change your License information.                                                                               |                 |
|                  | <b>About <i>Management_Application_Name</i>.</b> Select to view the application information, such as the company information and release number. |                 |

## Shortcut menus

You can use the Management application interface main menu to configure, monitor, and troubleshoot your SAN components. The instructions for using these features are documented in the subsequent chapters of this manual.

For each SAN component, you can optionally right-click the component and a shortcut menu displays. The table below details the command options available for each component.

| Component                           | Menu/Submenu Commands                                                                            | Comments                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <b>FC Fabric or Backbone Fabric</b> |                                                                                                  |                                                                                 |
|                                     | Zoning                                                                                           |                                                                                 |
|                                     | LSAN Zoning (Device Sharing)                                                                     | Only enabled for Backbone fabrics.                                              |
|                                     | Performance ><br>End-to-End Monitors<br>Real-Time Graph<br>Historical Graph<br>Historical Report |                                                                                 |
|                                     | Events                                                                                           |                                                                                 |
|                                     | Configure FCIP Tunnels                                                                           | Only launches the wizard when FCIP-capable switches are in the selected fabric. |
|                                     | High Integrity Fabric                                                                            |                                                                                 |
|                                     | Fabric Binding                                                                                   |                                                                                 |
|                                     | Router Configuration                                                                             |                                                                                 |
|                                     | Routing Domain IDs                                                                               |                                                                                 |
|                                     | Technical Support ><br>Switch/Host SupportSave<br>Upload Failure Data Capture<br>View Repository |                                                                                 |
|                                     | View ><br>Port List<br>Node List                                                                 |                                                                                 |
|                                     | Track Fabric Changes check box                                                                   |                                                                                 |
|                                     | Accept Changes                                                                                   |                                                                                 |

| Component           | Menu/Submenu Commands                                                                                                                                                               | Comments                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
|                     | Trace Route                                                                                                                                                                         |                                                                                                |
|                     | Connected End Devices ><br>Include Virtual Devices check box<br>Hide All<br>Show All<br>Custom<br>MyCustomList                                                                      |                                                                                                |
|                     | Create Meta SAN View                                                                                                                                                                | Only available for Backbone fabrics.                                                           |
|                     | Create View Automatically                                                                                                                                                           | Automatically creates a view with the selected fabric. View name is same as the current label. |
|                     | Map Display                                                                                                                                                                         |                                                                                                |
|                     | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                              | Only available from Product List.                                                              |
|                     | Collapse or Expand                                                                                                                                                                  | Only available from Connectivity Map                                                           |
|                     | Table ><br>Copy 'Fabric_Name'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List.                                                              |
|                     | Properties                                                                                                                                                                          |                                                                                                |
| <b>Device Group</b> |                                                                                                                                                                                     |                                                                                                |
|                     | Host Port Mapping                                                                                                                                                                   | Only available for servers or host group.                                                      |
|                     | Zoning                                                                                                                                                                              | Only available for switch group.                                                               |
|                     | Storage Port Mapping                                                                                                                                                                | Only available for storage group.                                                              |
|                     | Map Display                                                                                                                                                                         |                                                                                                |
|                     | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                              | Only available from Product List.                                                              |

## A Shortcut menus

| Component                                      | Menu/Submenu Commands                                                                                                                                                                                                                                 | Comments                                                                                                                                        |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize                                                             | Only available from Product List.                                                                                                               |
|                                                | Collapse or Expand                                                                                                                                                                                                                                    | Only available from Connectivity Map                                                                                                            |
| <b>Fabric OS Switch/Chassis/Access Gateway</b> |                                                                                                                                                                                                                                                       |                                                                                                                                                 |
|                                                | Element Manager ><br>Hardware<br>Ports<br>Admin<br>Router Admin                                                                                                                                                                                       |                                                                                                                                                 |
|                                                | Configuration ><br>Save<br>Save Running to Startup (CEE-capable switch)<br>Restore<br>CEE (CEE-capable switch)<br>FCoE (CEE-capable switch)<br>Schedule Backup<br>Configuration Repository<br>Replicate ><br>Configuration<br>Security<br>Swap Blades |                                                                                                                                                 |
|                                                | Firmware Management                                                                                                                                                                                                                                   |                                                                                                                                                 |
|                                                | Zoning                                                                                                                                                                                                                                                | Does not display when switch is in a Core Switch group, Chassis group or Isolated device group, or when it is in Access Gateway mode.           |
|                                                | Allow / Prohibit Matrix                                                                                                                                                                                                                               | Only available for Fabric OS devices.<br>Only enabled when the Fabric OS device is FICON-capable and has the Enhanced Group Management license. |
|                                                | Technical Support ><br>Switch/Host SupportSave<br>Upload Failure Data Capture<br>View Repository                                                                                                                                                      |                                                                                                                                                 |
|                                                | Port Connectivity                                                                                                                                                                                                                                     |                                                                                                                                                 |

| Component | Menu/Submenu Commands                                                                                                  | Comments                                                                                      |
|-----------|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|           | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections | Only available from Product List.                                                             |
|           | Port Optics (SFP)                                                                                                      |                                                                                               |
|           | Port Fencing                                                                                                           |                                                                                               |
|           | Performance ><br>Top Talkers<br>Clear Counters<br>Real-Time Graph<br>Historical Graph<br>Historical Report             |                                                                                               |
|           | Events                                                                                                                 |                                                                                               |
|           | Enable / Disable ><br>Enable<br>Disable                                                                                |                                                                                               |
|           | Telnet                                                                                                                 |                                                                                               |
|           | Telnet through Server                                                                                                  |                                                                                               |
|           | <User-defined menu item>                                                                                               | Configured in Setup Tools. May be more than one item.                                         |
|           | Setup Tools                                                                                                            |                                                                                               |
|           | Product                                                                                                                | Only enabled when the fabric is tracked, and the product is removed and joins another fabric. |
|           | Other Ports ><br><Fabric Name 1><br><Fabric Name 2>                                                                    | Does not display when an Access Gateway mode device is attached to multiple fabrics.          |
|           | Accept Change                                                                                                          | Only enabled in tracked FC Fabrics.<br>Only enabled when a plus or minus icon is present.     |
|           | Show Ports check box                                                                                                   |                                                                                               |
|           | Show Connections                                                                                                       |                                                                                               |
|           | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections | Only available from Product List.                                                             |

## A Shortcut menus

| Component                    | Menu/Submenu Commands                                                                                                                                                                     | Comments                                                                                      |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|                              | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List.                                                             |
|                              | Properties                                                                                                                                                                                |                                                                                               |
| <b>M-EOS Switch/Director</b> |                                                                                                                                                                                           |                                                                                               |
|                              | Zoning                                                                                                                                                                                    |                                                                                               |
|                              | Element Manager                                                                                                                                                                           |                                                                                               |
|                              | Performance ><br>Real-Time Graph<br>Historical Graph<br>Historical Report                                                                                                                 |                                                                                               |
|                              | Events                                                                                                                                                                                    |                                                                                               |
|                              | Port Connectivity                                                                                                                                                                         |                                                                                               |
|                              | Port Fencing                                                                                                                                                                              |                                                                                               |
|                              | Web Server                                                                                                                                                                                |                                                                                               |
|                              | <User-defined menu item>                                                                                                                                                                  | Configured in Setup Tools. May be more than one item.                                         |
|                              | Telnet                                                                                                                                                                                    | Disabled when the device does not have an IP address assigned or discovered.                  |
|                              | Telnet through Server                                                                                                                                                                     | Disabled when the device does not have an IP address assigned or discovered.                  |
|                              | Setup Tools                                                                                                                                                                               |                                                                                               |
|                              | Product                                                                                                                                                                                   | Only enabled when the fabric is tracked, and the product is removed and joins another fabric. |
|                              | Accept Change                                                                                                                                                                             |                                                                                               |
|                              | Show Ports                                                                                                                                                                                |                                                                                               |
|                              | Show Connections                                                                                                                                                                          |                                                                                               |
|                              | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List.                                                             |

| Component          | Menu/Submenu Commands                                                                                                                                                                     | Comments                          |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
|                    | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List. |
|                    | Properties                                                                                                                                                                                |                                   |
| <b>Core Switch</b> |                                                                                                                                                                                           |                                   |
|                    | Element Manager                                                                                                                                                                           | Only available from Product List. |
|                    | Enable/Disable Virtual Fabric (Fabric OS only)                                                                                                                                            | Only available from Product List. |
|                    | Logical Switches > <i>List_of_Logical_Switches</i><br>(Fabric OS only)                                                                                                                    | Only available from Product List. |
|                    | Configuration > (Fabric OS only)<br>Save<br>Restore<br>Schedule Backup<br>Configuration Repository<br>Replicate ><br>Configuration<br>Security<br>Swap Blades                             |                                   |
|                    | Firmware Management (Fabric OS only)                                                                                                                                                      |                                   |
|                    | Events                                                                                                                                                                                    |                                   |
|                    | Technical Support > (Fabric OS only)<br>Switch/Host SupportSave<br>Upload Failure Data Capture<br>View Repository                                                                         |                                   |
|                    | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List. |

## A Shortcut menus

| Component                                 | Menu/Submenu Commands                                                                                                                                                                     | Comments                                                                                                                    |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
|                                           | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List.                                                                                           |
|                                           | Properties                                                                                                                                                                                |                                                                                                                             |
| <b>HBA, iSCSI Host, and HBA Enclosure</b> |                                                                                                                                                                                           |                                                                                                                             |
|                                           | Element Manager                                                                                                                                                                           | Launches Element Manager for Brocade HBAs discovered using JSON agent.<br>Launches blank window for unmanaged Brocade HBAs. |
|                                           | Host Port Mapping                                                                                                                                                                         | Only available for Brocade, Emulex, and Qlogic HBAs.                                                                        |
|                                           | Performance ><br>Real Time Graphs                                                                                                                                                         | Disabled when all ports are offline.<br>Does not display for Node Origin and Routed instance in a routed fabric.            |
|                                           | Mapping Product                                                                                                                                                                           | Only available for Brocade HBAs.                                                                                            |
|                                           | LightPulse Utility/NT                                                                                                                                                                     | Only available for Emulex devices.<br>Launches with Origin in context for routed device.                                    |
|                                           | Emulex Configuration Tool                                                                                                                                                                 | Only available for Emulex devices.<br>Launches with Origin in context for routed device.                                    |
|                                           | SANSurfer                                                                                                                                                                                 | Only available for Qlogic HBAs.                                                                                             |
|                                           | <User-defined menu item>                                                                                                                                                                  | Configured in Setup Tools. May be more than one item.                                                                       |
|                                           | Host                                                                                                                                                                                      | Only available in Fabric view for managed HBAs.                                                                             |
|                                           | Setup Tools                                                                                                                                                                               |                                                                                                                             |
|                                           | Show Ports                                                                                                                                                                                |                                                                                                                             |
|                                           | Show Connections                                                                                                                                                                          |                                                                                                                             |
|                                           | Fabric ><br>Fabric1<br>Fabric2                                                                                                                                                            | Only available for HBAs under the Host node.                                                                                |
|                                           | Origin                                                                                                                                                                                    | Only available for HBAs under the Host node or devices routed in.<br>Not available for enclosures.                          |
|                                           | Destination                                                                                                                                                                               | Only available for devices routed out.<br>Not available for enclosures.                                                     |

| Component                                            | Menu/Submenu Commands                                                                                                                                                                     | Comments                                                                                     |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|                                                      | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List.                                                            |
|                                                      | Expand All                                                                                                                                                                                | Only available from Product List.                                                            |
|                                                      | Collapse All                                                                                                                                                                              | Only available from Product List.                                                            |
|                                                      | Properties                                                                                                                                                                                |                                                                                              |
| <b>Storage, iSCSI Storage, and Storage Enclosure</b> |                                                                                                                                                                                           |                                                                                              |
|                                                      | Storage Port Mapping                                                                                                                                                                      | Disabled for routed device.                                                                  |
|                                                      | <User defined menu item>                                                                                                                                                                  |                                                                                              |
|                                                      | Setup Tools                                                                                                                                                                               |                                                                                              |
|                                                      | Show Ports                                                                                                                                                                                |                                                                                              |
|                                                      | Show Connections                                                                                                                                                                          |                                                                                              |
|                                                      | Origin                                                                                                                                                                                    | Only available for devices routed in.<br>Not available for enclosures.                       |
|                                                      | Destination                                                                                                                                                                               | Only available for devices routed out.<br>Not available for enclosures.                      |
|                                                      | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List.                                                            |
|                                                      | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List.                                                            |
|                                                      | Properties                                                                                                                                                                                |                                                                                              |
| <b>Router Phantom Domains</b>                        |                                                                                                                                                                                           |                                                                                              |
|                                                      | Accept Change                                                                                                                                                                             | Only available for tracked FC Fabrics.<br>Only enabled when a plus or minus icon is present. |
|                                                      | Show Connections                                                                                                                                                                          | Displays as disabled because this component does not display in the Connectivity Map.        |
|                                                      | Origin                                                                                                                                                                                    |                                                                                              |

## A Shortcut menus

| Component      | Menu/Submenu Commands                                                                                                                                                                     | Comments                          |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
|                | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List. |
|                | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List. |
|                | Properties                                                                                                                                                                                |                                   |
| Switch Port FC |                                                                                                                                                                                           |                                   |
|                | Performance ><br>Real-Time Graph<br>Historical Graph<br>Historical Report                                                                                                                 |                                   |
|                | Zoning                                                                                                                                                                                    |                                   |
|                | List Zone Members                                                                                                                                                                         |                                   |
|                | Enable / Disable ><br>Enable<br>Disable                                                                                                                                                   |                                   |
|                | Connected Port                                                                                                                                                                            |                                   |
|                | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List. |
|                | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List. |
|                | Collapse All                                                                                                                                                                              | Only available from Product List. |

| Component                      | Menu/Submenu Commands                                                                                                                                                                     | Comments                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
|                                | Properties                                                                                                                                                                                |                                                                                                    |
| <b>HBA and iSCSI Initiator</b> |                                                                                                                                                                                           |                                                                                                    |
|                                | Performance ><br>Real Time Graphs                                                                                                                                                         | Disabled when all ports are offline.                                                               |
|                                | FC Security Protocol                                                                                                                                                                      | Only available for Managed JSON HBA Ports.<br>Only available when you have the Security Privilege. |
|                                | Zoning                                                                                                                                                                                    |                                                                                                    |
|                                | List Zone Members                                                                                                                                                                         |                                                                                                    |
|                                | Connected Port                                                                                                                                                                            |                                                                                                    |
|                                | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List.                                                                  |
|                                | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List.                                                                  |
|                                | Properties                                                                                                                                                                                |                                                                                                    |
| <b>HBA Port</b>                |                                                                                                                                                                                           |                                                                                                    |
|                                | Servers                                                                                                                                                                                   | Does not display for routed devices and discovered Hosts.                                          |
|                                | Performance ><br>Real Time Graphs                                                                                                                                                         | Only available for occupied, managed ports.<br>Disabled when all ports are offline.                |
|                                | FC Security Protocol                                                                                                                                                                      | Only available for Managed JSON HBA Ports.<br>Only available when you have the Security Privilege. |
|                                | Zoning                                                                                                                                                                                    |                                                                                                    |
|                                | List Zone Members                                                                                                                                                                         |                                                                                                    |
|                                | Connected Port                                                                                                                                                                            |                                                                                                    |
|                                | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List.                                                                  |
|                                | Expand All                                                                                                                                                                                | Only available from Product List.                                                                  |

## A Shortcut menus

| Component                                | Menu/Submenu Commands                                                                                                                                                                     | Comments                                                  |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
|                                          | Collapse All                                                                                                                                                                              | Only available from Product List.                         |
|                                          | Properties                                                                                                                                                                                |                                                           |
| <b>Storage Node</b>                      |                                                                                                                                                                                           |                                                           |
|                                          | Show Ports                                                                                                                                                                                | Does not display for routed devices and discovered Hosts. |
|                                          | Show Connections                                                                                                                                                                          |                                                           |
| <b>Storage FC and iSCSI Storage port</b> |                                                                                                                                                                                           |                                                           |
|                                          | Storage Port Mapping                                                                                                                                                                      |                                                           |
|                                          | Zoning                                                                                                                                                                                    |                                                           |
|                                          | List Zone Members                                                                                                                                                                         |                                                           |
|                                          | Connected Port                                                                                                                                                                            |                                                           |
|                                          | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List.                         |
|                                          | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List.                         |
|                                          | Properties                                                                                                                                                                                |                                                           |
| <b>Giga-Bit Ethernet Port</b>            |                                                                                                                                                                                           |                                                           |
|                                          | Performance ><br>Real-Time Graph                                                                                                                                                          |                                                           |
|                                          | Modify                                                                                                                                                                                    | Launches Element Manager.                                 |
|                                          | IP Troubleshooting ><br>Ping<br>Trace Route<br>Performance                                                                                                                                |                                                           |
|                                          | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List.                         |

| Component                          | Menu/Submenu Commands                                                                                                                                                                     | Comments                          |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
|                                    | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List. |
|                                    | Properties                                                                                                                                                                                |                                   |
| Connection                         |                                                                                                                                                                                           |                                   |
|                                    | Properties                                                                                                                                                                                |                                   |
| FCIP Tunnel                        |                                                                                                                                                                                           |                                   |
|                                    | Properties                                                                                                                                                                                |                                   |
| Trunk                              |                                                                                                                                                                                           |                                   |
|                                    | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                    | Only available from Product List. |
|                                    | Table ><br>Copy 'Device_Name Group'<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize | Only available from Product List. |
|                                    | Properties                                                                                                                                                                                |                                   |
| White Area of the Connectivity Map |                                                                                                                                                                                           |                                   |
|                                    | Zoom                                                                                                                                                                                      |                                   |
|                                    | Zoom In                                                                                                                                                                                   |                                   |
|                                    | Zoom Out                                                                                                                                                                                  |                                   |
|                                    | Map Display                                                                                                                                                                               |                                   |
|                                    | Expand                                                                                                                                                                                    |                                   |
|                                    | Collapse                                                                                                                                                                                  |                                   |
|                                    | Export                                                                                                                                                                                    |                                   |

A    Shortcut menus

| Component                      | Menu/Submenu Commands                                                                                                                                                                      | Comments                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| White Area of the Product List |                                                                                                                                                                                            |                                                                                          |
|                                | Port Display ><br>Occupied Product Ports<br>UnOccupied Product Ports<br>Attached Ports<br>Switch to Switch Connections                                                                     |                                                                                          |
|                                | Table ><br>Copy ' <i>Component</i> '<br>Copy Row<br>Copy Table<br>Export Row<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize |                                                                                          |
| Product List                   |                                                                                                                                                                                            |                                                                                          |
|                                | Table ><br>Copy ' <i>Component</i> '<br>Copy Table<br>Export Table<br>Search<br>Select All<br>Size All Columns To Fit<br>Expand All<br>Collapse All<br>Customize                           | Some form of this shortcut menu is available for all tables in the Management interface. |

# Call Home Event Tables

## In this appendix

This section provides information about the specific events that display when using Call Home. This information is shown in the following Event Tables.

- [Call Home Event Table . . . . .](#) 695
- [# CONSRV Events Table . . . . .](#) 697
- [# Thermal Event Reason Codes Table . . . . .](#) 697
- [# Brocade Events Table. . . . .](#) 698

## Call Home Event Table

| Event Reason Code | FRU Code / Event Type | Description                                                                | Severity |
|-------------------|-----------------------|----------------------------------------------------------------------------|----------|
| N/A               | Ethernet Event        | Management application unable to reach Switch.                             | 0        |
| N/A               | Ethernet Event        | Switch is not reachable.                                                   | 3        |
| N/A               | SW-Missing            | Switch is missing from Fabric.                                             | 3        |
| 10                | None/SW               | Login Server unable to synchronize databases.                              | 2        |
| 11                | None/SW               | Login Server database found to be invalid.                                 | 2        |
| 20                | None/SW               | Name Server unable to synchronize databases.                               | 2        |
| 21                | None/SW               | Name Server database found to be invalid.                                  | 2        |
| 40                | None/SW               | Operator panel has failed.                                                 | 2        |
| 50                | None/SW               | Management Server unable to synchronize databases.                         | 2        |
| 51                | None/SW               | Management Server database found to be invalid.                            | 2        |
| 60                | None/SW               | Fabric Controller unable to synchronize databases.                         | 2        |
| 61                | None/SW               | Fabric Controller database found to be invalid.                            | 2        |
| 82                | CTP/SW                | Port is blocked by port fencing.                                           | 0        |
| 86                | None/Info             | Continuous Incident detection and Reporting CIDR threshold value exceeded. | 0        |
| 90                | None/SW               | Database replication time out.                                             | 2        |
| 92                | BKP/HW                | Backplane NVRAM failure.                                                   | 3        |
| 200               | None/SW               | Power supply AC voltage failure.                                           | 3        |

## B Call Home Event Table

| Event Reason Code | FRU Code / Event Type | Description                                                 | Severity |
|-------------------|-----------------------|-------------------------------------------------------------|----------|
| 201               | PWR/HW                | Power supply DC voltage failure.                            | 3        |
| 202               | PWR/HW                | Power supply thermal failure.                               | 3        |
| 208               | PWR/HW                | Power supply false shutdown.                                | 3        |
| 210               | PWR/HW                | Power supply i2c bus failure.                               | 3        |
| 300               | FAN/HW                | A cooling fan propeller has failed.                         | 3        |
| 301               | FAN/HW                | A cooling fan propeller has failed (two failed propellers). | 3        |
| 302               | FAN/HW                | A cooling fan propeller has failed.                         | 3        |
| 303               | FAN/HW                | A cooling fan propeller has failed.                         | 3        |
| 304               | FAN/HW                | A cooling fan propeller has failed.                         | 3        |
| 305               | FAN/HW                | A cooling fan propeller has failed.                         | 3        |
| 306               | FAN/HW                | A cooling fan propeller in FAN2 FRU type has failed.        | 3        |
| 307               | FAN/HW                | A cooling fan propeller in FAN2 FRU type has failed.        | 3        |
| 322               | FAN/HW                | Front top fan FRU failed.                                   | 3        |
| 323               | FAN/HW                | Front bottom fan FRU failed.                                | 3        |
| 324               | FAN/HW                | Rear top fan FRU failed.                                    | 3        |
| 325               | FAN/HW                | Rear bottom fan FRU failed.                                 | 3        |
| 400               | CTP/HW                | Power-up diagnostic failure.                                | 3        |
| 411               | CTP/SW                | Firmware fault occurred.                                    | 3        |
| 413               | CTP/HW                | Backup CTP power-on self test failure.                      | 3        |
| 414               | CTP/HW                | Backup CTP failure.                                         | 3        |
| 419               | CTP/INFO              | Board NVRAM failure.                                        | 3        |
| 425               | CTP/HW                | CTP DRAM mismatch.                                          | 3        |
| 428               | CTP/HW                | CTP hardware component failure.                             | 3        |
| 433               | CTP/SW                | Non-recoverable Ethernet fault.                             | 3        |
| 440               | CTP/HW                | Embedded Port fatal error.                                  | 3        |
| 473               | CTP/SW                | CTP shutdown due to failure.                                | 3        |
| 483               | CTP/SW                | Partition shutdown due to failure.                          | 3        |
| 488               | CTP/HW                | Critical CTP failure on single CTP system.                  | 3        |

## # CONSRV Events Table

| Event Reason Code | FRU Code/Event Type | Description                                             | Severity |
|-------------------|---------------------|---------------------------------------------------------|----------|
| 504               | DVP/LIM/HW          | M-EOS: Port module failure.                             | 3        |
| 506               | DVP/PORT            | Fibre Channel port failure                              | 3        |
| 509               | DVP/PORT            | Fibre Channel path failure.                             | 0        |
| 511               | LIM/DVP             | LIM SPP failure.                                        | 3        |
| 514               | DVP/ LIM/PORT       | SFP/XFP optics failure.                                 | 3        |
| 517               | LIM                 | LIM SPP Offline.                                        | 3        |
| 530               | LIM/DVP             | LIM Power-up diagnostic failure.                        | 3        |
| 536               | LIM/DVP             | Internal Frame Error port anomaly - threshold exceeded. | 2        |
| 604               | SBAR/SWM/HW         | M-EOS: SBAR module failure.                             | 3        |
| 607               | SBAR/SWM/HW         | M-EOS: Switch contains no operational SBAR cards.       | 4        |
| 610               | SWM/INFO            | SWM BMAC Link Down.                                     | 0        |
| 622               | SBAR/INFO           | SWM powered off                                         | 0        |
| 625               | SBAR/INFO           | SWM NV RAM failure.                                     | 0        |

## # Thermal Event Reason Codes Table

| Event Reason Code | FRU Code/Event Type | Description                                              | Severity |
|-------------------|---------------------|----------------------------------------------------------|----------|
| 800               | DVP/LIM/HW          | High temperature warning.                                | 3        |
| 801               | DVP/LIM/HW          | Critically hot temperature warning.                      | 3        |
| 802               | DVP/LIM/HW          | M-EOS: Port card shutdown due to thermal violations.     | 3        |
| 805               | SWM/SBAR/HW         | High temperature warning.                                | 3        |
| 806               | SWM/SBAR/HW         | Critically hot temperature warning.                      | 3        |
| 807               | SWM/SBAR/HW         | M-EOS: SBAR module shutdown due to thermal violations.   | 3        |
| 810               | CTP/HW              | High temperature warning.                                | 3        |
| 811               | CTP/HW              | Critically hot temperature warning.                      | 3        |
| 812               | CTP/HW              | CTP shutdown due to thermal violations.                  | 3        |
| 850               | CTP/HW              | System shutdown due to CTP thermal threshold violations. | 4        |

## # Brocade Events Table

| Event Reason Code | FRU Code/Event Type | Description                                                    | Severity |
|-------------------|---------------------|----------------------------------------------------------------|----------|
| 1009              | MS-1009             | Error in registered link incident record (RLIR)                | 4        |
| 1402              | FW-1402             | Flash usage is out of range (Fabric OS version 6.0 or earlier) | 3        |
| 1426              | FW-1426             | Faulty or Missing Power supply                                 | 3        |
| 1427              | FW-1427             | Faulty Power supply                                            | 3        |
| 1428              | FW-1428             | Missing Power supply                                           | 3        |
| 1429              | FW-1429             | Problem in power supply arrangement                            | 3        |
| 1430              | FW-1430             | Faulty Temperature sensors                                     | 3        |
| 1431              | FW-1431             | Faulty fans                                                    | 3        |
| 1432              | FW-1432             | Faulty WWN Cards                                               | 3        |
| 1433              | FW-1433             | Faulty CPs                                                     | 3        |
| 1434              | FW-1434             | Faulty Blades                                                  | 3        |
| 1435              | FW-1435             | Flash usage is out of range (Fabric OS version 6.1 or later)   | 3        |
| 1436              | FW-1436             | Marginal port                                                  | 3        |
| 1437              | FW-1437             | Faulty Port                                                    | 3        |
| 1438              | FW-1438             | Faulty or Missing SFPs                                         | 3        |

# User Privileges

---

## In this appendix

- [About User Privileges. . . . .](#) 699
- [About Roles and Access Levels . . . . .](#) 717

## About User Privileges

The Management application provides the User Administrator with a high level of control over what functions individual users can see and use. This section describes the effect that each user privilege has on the application when placed in one of the three available configurations: no privilege, read-only, and read/write.

User privilege is the Management application's method of providing role-based access control (RBAC) to the software's user administrator.

In the Management application resource groups are assigned privileges, roles, and fabrics. Privileges are not directly assigned to users; users get privileges because they belong to a role in a resource group. A user can only belong to one resource group at a time.

The following table defines all the privileges in the Management application and the behavior of the application if the privilege is not given, read only, or read/write.

**TABLE 35** Privileges and Application Behavior

| Privilege                          | Description                                                                                           | No Privilege                                                                                                                                                                                                                                                                                                                                                                                          | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Read/Write                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active Session Management          | Allows you view active client sessions and disconnect an unwanted user.                               | Disables the <b>Active Sessions</b> command from the <b>Server</b> menu.                                                                                                                                                                                                                                                                                                                              | Enables the <b>Active Sessions</b> command from the <b>Server</b> menu.<br>Disables all commands and functions on the dialog box except the <b>Close</b> and <b>Help</b> .                                                                                                                                                                                                                                                                                 | Enables the <b>Active Sessions</b> command from the <b>Server</b> menu.<br>Enables all commands and functions on the dialog box.                                                                                                                                                                                                   |
| Add/Delete Properties              | Allows you to define new properties as well as remove them.                                           | Disables the <b>Add</b> , <b>Edit</b> and <b>Delete</b> buttons on the <b>Create View</b> dialog box <b>Columns</b> tab. Disables the <b>Add Column</b> , <b>Edit Column</b> , and <b>Delete Column</b> commands on the right-click menu of the <b>Product List</b> column headers.<br>Disables the <b>Add</b> , <b>Edit</b> , and <b>Delete</b> commands on the property headers in property sheets. | Same as No Privilege.                                                                                                                                                                                                                                                                                                                                                                                                                                      | Enables the <b>Add</b> , <b>Edit</b> , and <b>Delete</b> properties commands and buttons in the <b>Create View</b> and <b>Edit View</b> dialog boxes, the <b>Product List</b> column header right-click menu, and the Property Sheet property header right-click menu.                                                             |
| Backup                             | Allows you to control the function that copies (backs up) the application data files to another disk. | Disables the <b>Backup Now</b> and <b>Configure</b> commands on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the <b>Options</b> dialog box.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions.                                                            | Disables the <b>Configure</b> command on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the <b>Options</b> dialog box.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions.                                                                                                                                        | Enables the <b>Backup Now</b> and <b>Configure</b> commands on the Backup icon right-click menu on the application status bar. Enables all functions for Backup on the <b>Options</b> dialog box.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab and enables all functions. |
| Call Home Event Notification Setup | Allows you to configure call home centers, devices, and event filters.                                | Disables the <b>Advanced Call Home</b> command on the <b>Monitor &gt; Event Notification</b> menu.                                                                                                                                                                                                                                                                                                    | Enables the <b>Advanced Call Home</b> command on the <b>Monitor &gt; Event Notification</b> menu.<br>Enables the <b>Add</b> , <b>Edit</b> , <b>Remove</b> , <b>Edit Centers</b> , and <b>Show/Hide Centers</b> buttons as well as the <b>Enabled</b> check boxes on the dialog box; however, disables the <b>OK</b> and <b>Apply</b> buttons on the <b>Call Home</b> , <b>Call Home Event Filter</b> , and <b>Configure Call Home Center</b> dialog boxes. | Enables the <b>Advanced Call Home</b> command on the <b>Monitor &gt; Event Notification</b> menu.<br>Enables all functions in the dialog box.                                                                                                                                                                                      |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                    | Description                                                                                                           | No Privilege                                                                                                                                                                                                                     | Read-Only                                                                                                                                                                                                                                                                                                 | Read/Write                                                                                                                                                                                                                                                              |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CEE Management               | Allows you to configure CEE devices.                                                                                  | Disables the <b>Switch &gt; CEE</b> command from the <b>Configure</b> menu.                                                                                                                                                      | Enables the <b>Switch &gt; CEE</b> command from the <b>Configure</b> menu.<br>Disables all commands and functions on the dialog box except the <b>Close</b> , <b>Cancel</b> , and <b>Help</b> .                                                                                                           | Enables the <b>Switch &gt; CEE</b> command from the <b>Configure</b> menu.<br>Enables all commands and functions on the dialog box.                                                                                                                                     |
| Configuration Management     | Allows you to access the <b>Configuration Management</b> dialog box and perform configuration upload and replication. | Disables <b>Save</b> , <b>Restore</b> , <b>Configuration Repository</b> , and <b>Schedule Backup</b> under <b>Configure &gt; Switch</b> and the <b>Configuration</b> command under <b>Configure &gt; Switch &gt; Replicate</b> . | Enables <b>Configuration Repository</b> under <b>Configure &gt; Switch</b> .<br>Only viewing of saved configuration is supported.<br>Configuration upload and replication are disabled.                                                                                                                   | Enables all commands under <b>Configure &gt; Switch</b> .<br>Allows you to perform configuration upload, download and restore.                                                                                                                                          |
| Diagnose and Troubleshooting | Allows you to run device connectivity check, fabric device sharing check and trace route.                             | Disables the <b>Device</b> , <b>Fabric Device Sharing</b> , <b>Connectivity</b> and <b>Trace Route</b> commands under <b>Configure &gt; FC Troubleshooting</b> .                                                                 | Disables the <b>Device Connectivity</b> , <b>Fabric Device Sharing</b> , and <b>Trace Route</b> commands under <b>Configure &gt; FC Troubleshooting</b> .                                                                                                                                                 | Enables the <b>Device Connectivity</b> , <b>Fabric Device Sharing</b> , and <b>Trace Route</b> commands under <b>Configure &gt; FC Troubleshooting</b> .<br>Enables all functions in the dialog boxes.                                                                  |
| Discovery Setup              | Allows you to configure discovery setup.                                                                              | Disables <b>Setup</b> on the <b>Discover</b> menu and toolbar.<br>Enables you to launch <b>Discover Setup</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions.                    | Enables <b>Setup</b> on the <b>Discover</b> menu and toolbar.<br>Allows you to open the <b>Discover Setup</b> dialog box; however, disables all functions.<br>Enables you to launch <b>Discover Setup</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions. | Enables <b>Setup</b> on the <b>Discover</b> menu and toolbar.<br>Enables all functions in the <b>Discover Setup</b> dialog box.<br>Enables you to launch <b>Discover Setup</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab and enables all functions. |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                       | Description                                                                                                                                                      | No Privilege                                                                                                                                                                                                                                                                                                                                                                                                     | Read-Only                                                                                                                                                                                                                                                                               | Read/Write                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-mail Event Notification Setup | Allows you to define the e-mail server used to send e-mail.                                                                                                      | Disables <b>Event Notification E-mail</b> command on the <b>Monitor</b> menu and the <b>E-mail Event Notification Setup</b> button in the <b>Users</b> dialog box. Disables the <b>E-mail</b> option in the Master Log shortcut menu. Currently asks, "Are you sure you want to assign Event Management privileges to this group that does not otherwise have read/write for: E-mail Event Notification Setup?". | Enables the <b>Event Notification E-mail</b> command on the <b>Monitor</b> menu and the <b>E-mail Event Notification Setup</b> button in the <b>Users</b> dialog box. Allows you to open the <b>E-Mail Event Notification Setup</b> dialog box; however, disables the <b>OK</b> button. | Enables <b>Event Notification E-mail</b> command on the <b>Monitor</b> menu and the <b>E-mail Event Notification Setup</b> button in the <b>Users</b> dialog box. Enables all functions in the <b>E-Mail Event Notification Setup</b> dialog box. |
| Event Management                | Allows you to define rules with event triggers and actions.                                                                                                      | Disables the <b>Event Policies</b> menu item.                                                                                                                                                                                                                                                                                                                                                                    | Enables access to the <b>Event Policies</b> menu item and allows existing rules to be selected and viewed. Disables all action buttons on the tab.                                                                                                                                      | Enables access to the <b>Event Policies</b> menu item and enables all functions on the tab.                                                                                                                                                       |
| Fabric Binding                  | Allows you to define the switches allowed to join a fabric. Allows you to control access to the <b>Fabric Binding</b> dialog box from the <b>Configure</b> menu. | Disables the <b>Fabric Binding</b> command on the <b>Configure</b> menu.                                                                                                                                                                                                                                                                                                                                         | Enables the <b>Fabric Binding</b> command on the <b>Configure</b> menu; however, disables the <b>OK</b> button.                                                                                                                                                                         | Enables the <b>Fabric Binding</b> command on the <b>Configure</b> menu. Enables all functions in the dialog box.                                                                                                                                  |
| Fabric Tracking                 | Allows you to define the current devices and connections present in a fabric as a baseline and to highlight any changes to that baseline.                        | Disables the <b>Track Fabric Changes</b> and <b>Accept Changes</b> commands on the <b>Monitor</b> menu and right-click menus of <b>Fabrics</b> .                                                                                                                                                                                                                                                                 | Same as no privilege.                                                                                                                                                                                                                                                                   | Enables the <b>Track Fabric Changes</b> and <b>Accept Changes</b> commands on the <b>Monitor</b> menu and right-click menus of <b>Fabrics</b> .                                                                                                   |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege        | Description                                                                                                                                                                                                                                                                                                                                                                                                   | No Privilege                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Read/Write                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fault Management | Allows you to control access to the <b>SNMP Trap Registration and Forwarding</b> dialog box, the <b>Event Storage</b> option of the <b>Options</b> dialog box, the <b>Syslog Registration and Forwarding</b> dialog box, as well as the <b>Export</b> and <b>Clear</b> functions in the <b>Event Log</b> dialog box and the <b>Show</b> and <b>Hide</b> functions in the <b>Customize Columns</b> dialog box. | <p>Disables the <b>SNMP Trap</b> and <b>Syslog configuration</b> commands from the <b>Monitor</b> menu.</p> <p>Disables the <b>Event Storage</b> option on the <b>Options</b> dialog box.</p> <p>If you do not have other read/write privileges to <b>Options</b> dialog box functions, disables the <b>Server &gt; Options</b> command.</p> <p>Enables the <b>Logs &gt; Log_Type</b> from the <b>Monitor</b> menu.</p> <p>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions.</p> | <p>Enables the <b>SNMP Trap</b> and <b>Syslog configuration</b> commands from the <b>Monitor</b> menu.</p> <p>Enables the <b>Event Storage</b> option on the <b>Options</b> dialog box.</p> <p>Enables the <b>Server &gt; Options</b> command.</p> <p>Only enables the <b>Cancel</b> function for the dialog boxes.</p> <p>Enables the <b>Logs &gt; Log_Type</b> from the <b>Monitor</b> menu.</p> <p>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions.</p> | <p>Enables the <b>SNMP Trap</b> and <b>Syslog configuration</b> commands from the <b>Monitor</b> menu.</p> <p>Enables the following functions from the dialog boxes:</p> <ul style="list-style-type: none"> <li>configure Management server registration</li> <li>configure TRAP or Syslog forwarding</li> <li>register other servers as a recipient</li> <li>apply changes</li> </ul> <p>Enables the <b>Server &gt; Options</b> command.</p> <p>Enables the <b>Event Storage</b> option on the <b>Options</b> dialog box.</p> <p>Enables the following functions from the dialog box:</p> <ul style="list-style-type: none"> <li>configure max events</li> <li>configure event purging policy</li> <li>apply changes</li> </ul> <p>Enables the following functions from the <b>Master Log</b> right-click menu:</p> <ul style="list-style-type: none"> <li>Clear events</li> <li>Show events</li> <li>Hide events</li> <li>Export events</li> </ul> <p>Note that the <b>Export</b> command on the <b>Master Log</b> right-click menu also requires the <b>Export</b> privilege because it launches the <b>Export</b> dialog box.</p> <p>Enables the <b>Clear</b> and <b>Export</b> buttons on the individual log dialog boxes.</p> <p>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab and enables all functions.</p> |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege           | Description                                                                                                                                                                                                   | No Privilege                                                                                                                                                                                                                | Read-Only                                                                                                                                                                                                                                                                                                                                                                | Read/Write                                                                                                                                                                                                                                                                                          |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FCIP Management     | Allows you to configure FCIP tunnels and troubleshooting of IP interfaces (IP performance, IP ping and IP trace route).                                                                                       | Disables the <b>Configure &gt; FCIP Tunnel</b> and <b>Configure &gt; IP Troubleshooting</b> commands. Disables the <b>FCIP Tunnel</b> command on the Fabric right-click menu.                                               | Enables the <b>Configure &gt; FCIP Tunnel</b> and <b>Configure &gt; IP Troubleshooting</b> commands.<br><br>Only enables the <b>Cancel</b> function for the dialog boxes.                                                                                                                                                                                                | Enables the <b>Configure &gt; FCIP Tunnel</b> and <b>Configure &gt; IP Troubleshooting</b> commands.<br><br>Enables all commands and functions on the associated dialog boxes. Also enables all commands on the <b>FCIP Tunnels</b> tab in the device's <b>Properties</b> dialog box.               |
| FCoE Management     | Allows you to configure FCoE devices.                                                                                                                                                                         | Disables the <b>Switch &gt; FCoE</b> command from the <b>Configure</b> menu.                                                                                                                                                | Enables the <b>Switch &gt; FCoE</b> command from the <b>Configure</b> menu.<br><br>Disables all commands and functions on the dialog box except the <b>Close</b> , <b>Cancel</b> , and <b>Help</b> .                                                                                                                                                                     | Enables the <b>Switch &gt; FCoE</b> command from the <b>Configure</b> menu.<br><br>Enables all commands and functions on the dialog box.                                                                                                                                                            |
| FICON Management    | Allows you to configure Cascade FICON Fabric and Cascade FICON Fabric Merge.<br><br>Also allows you to configure block ports and allow/prohibit matrix on active configuration or any offline configurations. | Disables the <b>Configure Fabric</b> , <b>Merge Fabrics</b> commands on the <b>Configure &gt; FICON</b> menu.<br><br>Disables the <b>Allow/Prohibit Matrix</b> command from the <b>Configure</b> menu and right-click menu. | Disables the <b>Configure Fabric</b> , <b>Merge Fabrics</b> commands on the <b>Configure &gt; FICON</b> menu.<br><br>Enables the <b>Allow/Prohibit Matrix</b> command from the <b>Configure</b> menu and right-click menu.<br><br>Disables all commands and functions on the <b>Configure Allow/Prohibit Matrix</b> dialog box except the <b>Close</b> and <b>Help</b> . | Enables the <b>Configure Fabric</b> , <b>Merge Fabrics</b> commands on the <b>Configure &gt; FICON</b> menu.<br><br>Enables the <b>Allow/Prohibit Matrix</b> command from the <b>Configure</b> menu and right-click menu.<br><br>Enables all commands and functions on the associated dialog boxes. |
| Firmware Management | Allows you to download firmware to selected switches and manage the firmware repository.                                                                                                                      | Disables the <b>Firmware Management</b> command from the <b>Configure</b> menu and right-click menu.                                                                                                                        | Enables the <b>Firmware Management</b> command from the <b>Configure</b> menu and right-click menu.<br><br>Disables all commands and functions on the dialog box except the <b>Close</b> and <b>Help</b> .                                                                                                                                                               | Enables the <b>Firmware Management</b> command from the <b>Configure</b> menu and right-click menu.<br><br>Enables all commands and functions on the dialog box.                                                                                                                                    |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                    | Description                                                                                                                                                                                                                                                                                              | No Privilege                                                                                                                                      | Read-Only                                                                                                                                                                                                                                        | Read/Write                                                                                                                                                                                                                                     |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High Integrity Fabric        | For Fabric OS devices, allows you to set Fabric Binding and Insistent Domain IDs.<br>For M-EOS devices, allows you to activate the High Integrity Fabric, which activates Fabric Binding, Switch Binding, Insistent Domain ID, Rerouting Delay, and Domain RSCNs.                                        | Disables the <b>High Integrity Fabric</b> command from the <b>Configure</b> menu.                                                                 | Enables the <b>High Integrity Fabric</b> command from the <b>Configure</b> menu.<br>Disables all commands and functions on the dialog box except the <b>Cancel</b> and <b>Help</b> .                                                             | Enables the <b>High Integrity Fabric</b> command from the <b>Configure</b> menu.<br>Disables all commands and functions on the dialog box.                                                                                                     |
| Host Management              | Allows you to configure a host.                                                                                                                                                                                                                                                                          | Disables the <b>Element Manager</b> command on the right-click menu and the <b>Element Manager &gt; HCM</b> command on the <b>Configure</b> menu. | Disables the <b>Element Manager</b> command on the right-click menu and the <b>Element Manager &gt; HCM</b> command on the <b>Configure</b> menu.                                                                                                | Enables the <b>Element Manager</b> command on the right-click menu and the <b>Element Manager &gt; HCM</b> command on the <b>Configure</b> menu.                                                                                               |
| License Update               | Allows you to update your license.<br>Allows you to control access to the <b>License</b> dialog box from the <b>Help</b> menu.                                                                                                                                                                           | Disables the <b>License</b> command on the <b>Help</b> menu.                                                                                      | Enables the <b>License</b> command on the <b>Help</b> menu; however, disables the <b>Update</b> and <b>OK</b> buttons.                                                                                                                           | Enables the <b>License</b> command on the <b>Help</b> menu and enables you to change the license key.                                                                                                                                          |
| Logical Switch Configuration | Allows you to create a new logical switch, assign and remove ports from a logical switch, delete a logical switch, configure a logical fabric, and change the fabric ID of a logical switch.<br>You must be assigned to the 'All Fabrics' resource group to access Logical Switch Configuration feature. | Disables the <b>Logical Switches</b> command from the <b>Configure</b> menu.                                                                      | Enables the <b>Logical Switches</b> command from the <b>Configure</b> menu.<br>Disables all functions from the dialog box except view.<br>Also requires access to All Resources resource group to access the <b>Logical Switches</b> dialog box. | Enables the <b>Logical Switches</b> command from the <b>Configure</b> menu.<br>Enables all commands and functions on the dialog box.<br>Also requires access to All Resources resource group to access the <b>Logical Switches</b> dialog box. |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege           | Description                                                                                                                                                                                                                                                                                                                                                | No Privilege                                                                                                                                                                                                                    | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Read/Write                                                                                                                                                                                                                             |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LSAN Zoning         | <p>Allows you to edit and activate LSAN zones for the LSAN fabrics that are available within the <b>Zoning</b> dialog box.</p> <p>Prerequisite:<br/>Both the backbone fabrics as well as all directly connected edge fabrics must be added to a resource group and a user with LSAN Zoning privilege must be assigned to this specific resource group.</p> | <p>Disables the <b>Zoning &gt; LSAN Zoning (Device Sharing)</b> command on the <b>Configure</b> menu.</p> <p>In <b>Zoning</b> dialog box, the <b>Zoning Scope</b> list does not include <i>LSAN_FabricName</i> as an entry.</p> | <p>Enables the <b>Zoning &gt; LSAN Zoning (Device Sharing)</b> command on the <b>Configure</b> menu.</p> <p>In <b>Zoning</b> dialog box, the <b>Zoning Scope</b> list includes <i>LSAN_FabricName</i> as an entry, if discovered. If <i>LSAN_FabricName</i> is selected, LSAN zone contents are loaded into the <b>Zoning</b> dialog box.</p> <p>Disables LSAN zone functions on all dialog boxes.</p> <p>Disables all online zone database editing, activation, and persisting functions.</p> <p>In <b>Zoning</b> dialog box, enables the <b>Cancel</b> and <b>Help</b> buttons.</p> <p>In the <b>Potential Members</b> table, enables all functions in the right-click menu.</p> <p>In the <b>LSAN Zones</b> table, enables the <b>Search</b> functions in the right-click menu.</p> | <p>Enables all LSAN zone functions on all dialog boxes.</p>                                                                                                                                                                            |
| Map Port to Storage | <p>Allows you to construct multi-port storage systems out of individual storage ports.</p>                                                                                                                                                                                                                                                                 | <p>Disables the <b>Storage Port Mapping</b> command from <b>Discover</b> menu and right-click menus for Storage products and ports in the tree and map.</p>                                                                     | <p>Enables the <b>Storage Port Mapping</b> command from <b>Discover</b> menu right-click menus for Storage products and ports in the tree and map.</p> <p>Allows you to open the <b>Storage Port Mapping</b> dialog box; however, disables the <b>Create</b>, <b>Delete</b>, right and left arrow, and <b>OK</b> buttons.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <p>Enables the <b>Storage Port Mapping</b> command from <b>Discover</b> menu and right-click menus for Storage products and ports in the tree and map.</p> <p>Enables all functions on the <b>Storage Port Mapping</b> dialog box.</p> |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege              | Description                                                                                                   | No Privilege                                                                                                                                                                                                                                                                                                           | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Read/Write                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Performance            | Allows you to configure the performance subsystem, the display of performance graphs, and threshold settings. | Disables entire <b>Performance</b> submenu of the <b>Monitor</b> menu as well as the right-click <b>Performance Graph(s)</b> command on ports and switch products. Disables the <b>Port Optics</b> command on the right-click menu. Disables the <b>Performance</b> button in the <b>CEE Configuration</b> dialog box. | Enables entire <b>Performance</b> submenu off the <b>Monitor</b> menu as well as the right-click <b>Performance Graph(s)</b> command on ports and switch products. Allows you to open the <b>Performance Setup</b> dialog box; however, disables the <b>OK</b> button. No changes can be made. Allows you to open the <b>Performance Graphs</b> dialog box and enables all controls; however, disables the check boxes under the <b>Set Thresholds</b> label on the individual port dialog box (double-click a graph). | Enables entire <b>Performance</b> submenu of the <b>Monitor</b> menu and the right-click <b>Performance Graph(s)</b> command on ports and switch products. Enables changes to the <b>Performance Setup</b> dialog box. Allows you to open the <b>Performance Graphs</b> dialog box and enables all controls. Enables all functions on the individual port dialog box (double-click a graph). Enables the <b>Port Optics</b> command on the right-click menu. |
| Port Fencing           | Allows you to configure the function that logs ports out of fabrics automatically if they are misbehaving.    | Disables the <b>Port Fencing</b> command from the <b>Configure</b> menu.                                                                                                                                                                                                                                               | Enables the <b>Port Fencing</b> command from the <b>Configure</b> menu. Disables the Thresholds <b>Add</b> , <b>Edit</b> , and <b>Delete</b> buttons, the right- and left-arrow threshold assignment buttons, and the <b>Port Unblock</b> and <b>Properties</b> buttons, and the <b>OK</b> button on the <b>Port Fencing</b> dialog box.                                                                                                                                                                               | Enables the <b>Port Fencing</b> command from the <b>Configure</b> menu. Enables all functions on the <b>Port Fencing</b> dialog box.                                                                                                                                                                                                                                                                                                                         |
| Product Administration | An Element Manager privilege that enables most functionally.                                                  | Disables the functions described in the <i>Element Manager User Manual</i> for which you do not have rights. Displays the message, "You do not have rights to perform this action." For Fabric OS devices, the log in dialog box for the switch displays.                                                              | Same as No Privilege.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Enables the functions described in the <i>Element Manager User Manual</i> .                                                                                                                                                                                                                                                                                                                                                                                  |

**NOTE**

This privilege affects M-EOS and M-EOSn switch product Element Managers.

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                                                                                                      | Description                                                      | No Privilege                                                                                                                                                                                                                                                    | Read-Only                                                                                                                                                                                                                                                                                     | Read/Write                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Maintenance<br><b>NOTE</b><br>This privilege affects M-EOS and M-EOSn switch product Element Managers. | An Element Manager privilege that enables maintenance functions. | Disables the functions described in the <i>Element Manager User Manual</i> for which you do not have rights.<br>Displays the message, "You do not have rights to perform this action."<br>For Fabric OS devices, the log in dialog box for the switch displays. | Same as No Privilege.                                                                                                                                                                                                                                                                         | Enables the functions described in the <i>Element Manager User Manual</i> .                                                                                                                                                                                                                           |
| Product Operation<br><b>NOTE</b><br>This privilege affects M-EOS and M-EOSn switch product Element Managers.   | An Element Manager privilege that enables operator functions.    | Disables the functions described in the <i>Element Manager User Manual</i> for which you do not have rights.<br>Displays the message, "You do not have rights to perform this action."<br>For Fabric OS devices, the log in dialog box for the switch displays. | Same as No Privilege.                                                                                                                                                                                                                                                                         | Enables the functions described in the <i>Element Manager User Manual</i> .                                                                                                                                                                                                                           |
| Properties Edit                                                                                                | Allows you to edit many director and switch properties.          | Enables the <b>Properties</b> command on <b>Edit</b> menu and right-click menus.<br>Disables edit function (removes green triangles) from editable property fields.<br>Disables the <b>Names</b> command on the <b>Configure</b> menu.                          | Enables the <b>Properties</b> command on <b>Edit</b> menu and right-click menus.<br>Disables edit function (removes green triangles) from editable property fields.<br>Enables the <b>Names</b> command on the <b>Configure</b> menu; however, disables all edit functions in the dialog box. | Enables <b>Properties</b> command on <b>Edit</b> menu and right-click menus.<br>Enables editable properties (marked by a green triangle) in the Product List and the Properties Sheets.<br>Enables the <b>Names</b> command on the <b>Configure</b> menu and enables all functions in the dialog box. |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege             | Description                                                                                                                                   | No Privilege                                                                                                                                                                                                                                                                                                                                                                                                                                         | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                       | Read/Write                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Report                | Allows you to generate and view the following reports: <ul style="list-style-type: none"> <li>Fabric Ports</li> <li>Fabric Summary</li> </ul> | Disables the <b>View</b> command and the <b>Generate</b> command on the <b>Reports</b> menu.<br>If this privilege is removed and the Event Management privilege is assigned then this message appears:<br><title: <Product><br>Message><br><Warning>Removing the Report privilege does not remove users' ability to generate reports in Event Management. You might also want to consider removing the Event Management privilege as well.<br><<OK>> | Enables the <b>View</b> command on the <b>Reports</b> menu.<br>Disables the <b>Generate</b> command on the <b>Reports</b> menu.                                                                                                                                                                                                                                                                                                                 | Enables the <b>View</b> command and the <b>Generate</b> command on the <b>Reports</b> menu.                                                                                                                                                                                                                                                                                                                                                          |
| Routing Configuration | Allows you to configure Routing and domain IDs of phantom switches.                                                                           | Disables the <b>Routing Configuration</b> and <b>Routing Domain IDs</b> commands from the <b>Configure</b> menu and right-click menu.                                                                                                                                                                                                                                                                                                                | Disables the <b>Routing Configuration</b> and <b>Routing Domain IDs</b> commands from the <b>Configure</b> menu and right-click menu.                                                                                                                                                                                                                                                                                                           | Enables the <b>Routing Configuration</b> and <b>Routing Domain IDs</b> commands from the <b>Configure</b> menu and right-click menu.<br>Enables all functions in the dialog boxes.                                                                                                                                                                                                                                                                   |
| Security              | Allows you to enable and configure SANtegrity features.                                                                                       | Disables the <b>Security</b> command from the <b>Configure &gt; Switch &gt; Replicate</b> menu.<br>Disables the <b>Security Log</b> command on the <b>Monitor &gt; Logs</b> menu.<br>Disables the <b>Security Misc</b> command from the <b>Server &gt; Options</b> menu.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions.                                     | Disables the <b>Security</b> command from the <b>Configure &gt; Switch &gt; Replicate</b> menu.<br>Enables the <b>Security Log</b> command on the <b>Monitor &gt; Logs</b> menu.<br>Enables the <b>Security Misc</b> command from the <b>Server &gt; Options</b> menu; however, disables the functions.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions. | Enables the <b>Security</b> command from the <b>Configure &gt; Switch &gt; Replicate</b> menu.<br>Enables the <b>Security Log</b> command on the <b>Monitor &gt; Logs</b> menu.<br>Enables the <b>Security Misc</b> command from the <b>Server &gt; Options</b> menu.<br>Enables all functions in the dialog boxes.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab and enables all functions. |
| Servers               | Allows you to identify all the HBAs that are in the same server.                                                                              | Disables the <b>Servers</b> command from the <b>Discover</b> menu.<br>Disables the <b>Server</b> right-click command on HBAs.                                                                                                                                                                                                                                                                                                                        | Enables <b>Servers</b> command from the <b>Discover</b> menu and right-click menu; however, disables the <b>Create</b> , <b>Delete</b> , and <b>OK</b> buttons.                                                                                                                                                                                                                                                                                 | Enables <b>Servers</b> command from the <b>Discover</b> menu and right-click menu.<br>Enables all functions in the <b>Servers</b> dialog box.                                                                                                                                                                                                                                                                                                        |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege       | Description                                                                                                      | No Privilege                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Read/Write                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Setup Tools     | Allows you to define and place commands on product icons and in the <b>Tools</b> menu.                           | Disables the <b>Setup Tools</b> command on the <b>Tools</b> menu. Any existing <b>Tools</b> and/or right-click commands already defined or defined by others are available for use; however, you cannot configure new items. If this privilege is removed and the Event Management privilege is assigned then this message appears:<br><title: <Product> Message><br><Warning>Removing the Log Management privilege does not remove users' ability for Setup Tools in Event Management. You might also want to consider removing the Event Management privilege as well. | Enables the <b>Setup Tools</b> command on the <b>Tools</b> menu; however, disables the <b>OK</b> button.                                                                                                                                                                                                                                                                                                                                                                                                      | Enables the <b>Setup Tools</b> command on the <b>Tools</b> menu.<br>Enables all functions in the <b>Setup Tools</b> dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SMIA Operations | Allows you to access the CIMOM (Common Information Model Object Manager) server and the SMIA Configuration Tool. | Enables the <b>Configure SMI Agent</b> button from the Server Console. Disables the <b>CIMOM</b> and <b>Certificate Management</b> tabs on the <b>SMIA Configuration Tool</b> dialog box. Denies access to the CIMOM server with the following WBEM exception<br>"CIM_ERR_ACCESS_DENIED: The specified principal does not have access to perform this operation". Allows you to retrieve all interop namespace information and retrieve getclass operation.                                                                                                              | Enables the <b>Configure SMI Agent</b> button from the Server Console. Enables the SMIA Configuration Tool Java web start application. However, disables all functions in the dialog box. Disables the <b>CIMOM</b> and <b>Certificate Management</b> tabs on the <b>SMIA Configuration Tool</b> dialog box. Allows access to the CIMOM server; however, denies changes with the following WBEM exception<br>"CIM_ERR_ACCESS_DENIED: The specified principal does not have access to perform this operation". | Enables the <b>Configure SMI Agent</b> button from the Server Console. Enables the SMIA Configuration Tool Java web start application. Enables all functions in the dialog box. Allows read and write access to the CIMOM server. If your password is changed by another user while logged into the CIMOM server, you continue to have read and write access until the Management server expires your session. Resource grouping is not applicable when filtering out Indications. You receive Indications from all fabrics managed by the CIMOM server regardless of resource groups by user. |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                         | Description                                                                                                                                                                                                                                                     | No Privilege                                                                                                                                                                                                                                                                            | Read-Only                                                                                                                                                                                                                                                                                                                                          | Read/Write                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Software Configuration Parameters | Allows you to configure some of the properties of the client and server of the management application.                                                                                                                                                          | Disables the <b>Software Configuration Parameters</b> folder and subpages in the <b>Options</b> dialog box. The configuration cannot be viewed.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions. | Enables the <b>Software Configuration Parameters</b> folder and subpages in the <b>Options</b> dialog box; however, disables the <b>OK</b> and <b>Apply</b> buttons when any of the subpages are selected.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab; however, disables all functions. | Enables the <b>Software Configuration Parameters</b> folder and subpages in the <b>Options</b> dialog box. Enables all functions when any of those subpages are selected.<br>Enables you to launch <b>Options</b> dialog box from the <b>SMIA Configuration Tool - Home</b> tab and enables all functions.                                                                                                                                                                    |
| Storage Encryption Configuration  | Allows you to configure storage encryption configuration, including selecting storage devices and LUNs, viewing and editing switch, group, or engine properties, viewing and editing storage device encryption properties, and initiating manual LUN re-keying. | Disables the <b>Encryption</b> command from the <b>Configure</b> menu.                                                                                                                                                                                                                  | Enables the <b>Encryption</b> command from the <b>Configure</b> menu.<br>Disables all functions from the dialog box except view.                                                                                                                                                                                                                   | Enables the <b>Encryption</b> command from the <b>Configure</b> menu.<br>Enables the following functions from the dialog box: <ul style="list-style-type: none"> <li>viewing and editing switch, group, or engine properties</li> <li>viewing and editing storage device encryption properties</li> <li>selecting storage devices and LUNs</li> <li>initiating manual LUN re-keying.</li> </ul> Disables all other functions from the <b>Configure Encryption</b> dialog box. |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                        | Description                                                                                                                                                                                                                                                                                                                                       | No Privilege                                                           | Read-Only                                                                                                                        | Read/Write                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Encryption Key Operation | Allows you to configure storage encryption key operation, including selecting storage devices and LUNs, viewing switch, group, or engine properties, viewing storage device encryption properties, initiating manual LUN re-keying, enabling and disabling an engine, zeroizing an engine, restoring a Master Key, and all smart card operations. | Disables the <b>Encryption</b> command from the <b>Configure</b> menu. | Enables the <b>Encryption</b> command from the <b>Configure</b> menu.<br>Disables all functions from the dialog box except view. | Enables the <b>Encryption</b> command from the <b>Configure</b> menu.<br>Enables the following functions from the dialog box: <ul style="list-style-type: none"> <li>viewing switch, group, or engine properties</li> <li>viewing storage device encryption properties</li> <li>selecting storage devices and LUNs</li> <li>initiating manual LUN re-keying.</li> <li>enabling and disabling an engine</li> <li>zeroizing an engine</li> <li>restoring a Master Key</li> <li>all smart card operations</li> </ul> Disables all other functions from the <b>Configure Encryption</b> dialog box. |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                         | Description                                                                                                                                                                                                                                                        | No Privilege                                                                                                                                                                                       | Read-Only                                                                                                                                                                                                                                                                         | Read/Write                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Encryption Security       | Allows you to configure storage encryption security, including creating a new encryption group, adding a switch to an existing group, zeroizing an encryption engine, backing up or restoring a master key, and enabling encryption functions after a power cycle. | Disables all functions from the dialog box except view.<br>The <b>Encryption</b> command from the <b>Configure</b> menu is enabled and disabled by the Storage Encryption Configuration privilege. | Disables all functions from the dialog box except view.<br>The <b>Encryption</b> command from the <b>Configure</b> menu is enabled and disabled by the Storage Encryption Configuration privilege.                                                                                | Enables the <b>Encryption</b> command from the <b>Configure</b> menu.<br>Enables the following functions from the dialog box: <ul style="list-style-type: none"> <li>creating a new encryption group</li> <li>adding a switch to an existing group</li> <li>zeroizing an encryption engine</li> <li>backing up or restoring a master key</li> <li>enabling encryption functions after a power cycle</li> <li>changing key vaults for an encryption group.</li> <li>create/edit/delete High Availability (HA) Clusters.</li> <li>removing switches from encryption groups.</li> <li>enable/disable encryption engines.</li> <li>create new master keys (backup and restore of master keys is already listed)</li> </ul> |
| Technical Support Data Collection | Allows you to capture support data from Fabric OS switches.                                                                                                                                                                                                        | Disables the <b>SupportSave</b> , <b>Upload Failure Data Capture</b> , and <b>View Repository</b> commands from the <b>Monitor &gt; Technical Support</b> menu and right-click menu.               | Enables the <b>View Repository</b> command from the <b>Monitor &gt; Technical Support</b> menu and right-click menu.<br>Disables the <b>SupportSave</b> and <b>Upload Failure Data Capture</b> commands from the <b>Monitor &gt; Technical Support</b> menu and right-click menu. | Enables the <b>SupportSave</b> , <b>Upload Failure Data Capture</b> , and <b>View Repository</b> commands from the <b>Monitor &gt; Technical Support</b> menu and right-click menu.<br>Enables all functions on the dialog boxes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                                                                                                                                                                        | Description                                                                                                                                                                                      | No Privilege                                                                                                                                                                                                                                                                                                                                                          | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                   | Read/Write                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Management                                                                                                                                                                  | Allows you to create and define users and groups, as well as assign privileges and views to groups.                                                                                              | Disables the <b>Users</b> command on the main <b>Server</b> menu and the <b>Users</b> button on the main tool bar.                                                                                                                                                                                                                                                    | Enables the <b>Users</b> command on the <b>Server</b> menu and the <b>Users</b> button on the main tool bar; however, disables the <b>Add</b> , <b>Edit</b> , and <b>Remove Users</b> , <b>Add and Remove Groups</b> , and <b>OK</b> buttons on the <b>Users</b> dialog box. Enables the <b>Edit Groups</b> button to display the <b>Group</b> dialog box (with <b>OK</b> button disabled).                                                 | Enables the <b>Users</b> command on the <b>Server</b> menu and the <b>Users</b> button on the main tool bar. Enables all functions on the <b>Users</b> dialog box and the secondary <b>Group</b> dialog box. |
| View Management                                                                                                                                                                  | Allows you to create, edit, and delete views. Selecting from views should always be allowed unless restricted by the assignment of Views in the Group definition in the <b>Users</b> dialog box. | Disables the <b>Create View</b> , <b>Copy View</b> , <b>Edit View</b> , <b>Delete View</b> , and <b>Connectivity View</b> commands in the <b>View &gt; Manage View</b> menu and the first tab header on the main desktop. Allows you to select an assigned view but not create or change. Disables the <b>Create View Automatically</b> command in the shortcut menu. | Enables the <b>Create View</b> and <b>Edit View</b> commands in the <b>View &gt; Manage View</b> menu and the first tab header on the main desktop; however, disables the <b>OK</b> button in the <b>Create View</b> and <b>Edit View</b> dialog boxes. Disables the <b>Copy View</b> , <b>Delete View</b> , and <b>Connectivity View &gt; Create and Refresh</b> commands. Allows you to select an assigned view but not create or change. | Activates all view commands in the <b>View &gt; Manage View</b> menu and the first tab header on the main desktop. Enables all functions in the dialog boxes.                                                |
| View Port Connectivity                                                                                                                                                           | Allows you to view all of the port details and connected devices.                                                                                                                                | Disables the <b>Port Connectivity</b> command from the <b>Monitor</b> menu and right-click menu.                                                                                                                                                                                                                                                                      | Enables the <b>Port Connectivity</b> command from the <b>Monitor</b> menu and right-click menu.                                                                                                                                                                                                                                                                                                                                             | Enables the <b>Port Connectivity</b> command from the <b>Monitor</b> menu and right-click menu.                                                                                                              |
| Zoning Activation (Fabric and offline zone database)                                                                                                                             | Allows you to activate a zone configuration selected in the <b>Zoning</b> dialog box.                                                                                                            | Disables the <b>Activate</b> , <b>Deactivate</b> , and <b>Zoning Policies</b> buttons in the <b>Zoning</b> dialog box.                                                                                                                                                                                                                                                | Enables the <b>Zoning Policies</b> button; however, you cannot perform any operations within the <b>Zoning</b> dialog box. Disables the <b>Activate</b> and <b>Deactivate</b> buttons in the <b>Zoning</b> dialog box.                                                                                                                                                                                                                      | Enables the <b>Activate</b> , <b>Deactivate</b> , and <b>Zoning Policies</b> buttons in the <b>Zoning</b> dialog box.                                                                                        |
| <b>NOTE</b><br>You must also have the Zoning Offline and Zoning Online privileges to launch the <b>Zoning</b> dialog box.                                                        |                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                              |
| <b>NOTE</b><br>You must also have the LSAN privilege to launch the <b>Activate LSAN Zones</b> dialog box from the <b>Zone Database (DB)</b> tab of the <b>Zoning</b> dialog box. |                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                              |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                                                                                                                                                                                                                                                                                                                                                         | Description                                                                                                         | No Privilege                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Read/Write                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Zoning Offline<br><hr/> <b>NOTE</b><br>You must also have the Zoning Activation privilege to enable the Activate button.<br><hr/> <b>NOTE</b><br>You must also have the Zoning g Online privilege to enable the <b>Save to Switch, Activate, Deactivate, and Rollback</b> functions in the <b>Zoning</b> dialog box and the <b>Save Compare/Merge</b> dialog box. | Allows you to edit the zone database in offline mode and save the zone database to the repository or to the switch. | In <b>Zoning</b> dialog box, the <b>Zone DB</b> list includes offline zones; however, if an offline zone is selected, the contents are not loaded into the <b>Zoning</b> dialog box.<br>Only displays the Fabric Zone DB (if you have the Zoning Online privilege) in the <b>Zone DB</b> list.<br>Disables the <b>Save As</b> function from <b>Zone DB Operation</b> list for Fabric Zone DBs.<br>Disables the <b>Save To</b> function on the <b>Active Zone Config</b> tab. | In <b>Zoning</b> dialog box, the <b>Zone DB</b> list includes offline zones. If you select an offline zone, the contents are loaded into the <b>Zoning</b> dialog box.<br>Disables all offline zone DB editing, activating, and persisting functions.<br>In <b>Zoning</b> dialog box, enables the <b>Cancel</b> and <b>Help</b> buttons and the <b>Compare</b> and <b>Export</b> functions in the <b>Zone DB Operation</b> list.<br>On the <b>Zone DB</b> tab, enables the find buttons.<br>On the <b>Active Zone Config</b> tab, enables the <b>Zone Member Display</b> list and <b>Report</b> button.<br>In the <b>Compare/Merge</b> dialog box, enables the <b>Cancel</b> and <b>Help</b> buttons.<br>In the <b>Potential Members</b> table, enables all functions in the right-click menu.<br>In the <b>Zones</b> table, enables the <b>Port Label, Search, and Properties</b> (not editable) functions in the right-click menu.<br>In the <b>Zone Configs</b> table, enables the <b>Properties</b> (not editable) function in the right-click menu. | Enables all functions on the <b>Zoning</b> dialog box. |

**TABLE 35** Privileges and Application Behavior (Continued)

| Privilege                                                                                                                                                                                                                                                                                                                         | Description                                                                                                                                                               | No Privilege                                                                                                                                                                                                                                                                                                                                      | Read-Only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Read/Write                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Zoning Online</p> <hr/> <p><b>NOTE</b><br/>You must also have the Zoning Activation privilege to enable the Activate button.</p> <hr/> <p><b>NOTE</b><br/>You must also have the Zoning g Offline privilege to enable the <b>Save As</b> function in the in the <b>Zoning</b> and <b>Compare/Merge</b> dialog boxes.</p> <hr/> | <p>Allows you to edit any of the fabric zone databases in the available fabrics within the <b>Zoning</b> dialog box from the client side and then save to the switch.</p> | <p>In <b>Zoning</b> dialog box, the <b>Zone DB</b> list includes online and offline zones; however, if an online zone is selected, the contents are not loaded into the <b>Zoning</b> dialog box. To launch offline zones you must have the Zoning Offline privilege.</p> <p>Disables all zone database editing and switch pushing functions.</p> | <p>In <b>Zoning</b> dialog box, the <b>Zone DB</b> list includes online and offline zones. If you select an online zone, the contents are loaded into the <b>Zoning</b> dialog box. To launch offline zones you must have the Zoning Offline privilege.</p> <p>Disables all online zone database editing, activation, and persisting functions.</p> <p>In <b>Zoning</b> dialog box, enables the <b>Cancel</b> and <b>Help</b> buttons and the <b>Compare</b> and <b>Export</b> functions in the <b>Zone DB Operation</b> list.</p> <p>On the <b>Zone DB</b> tab, enables the find buttons.</p> <p>On the <b>Active Zone Config</b> tab, enables the <b>Zone Member Display</b> list and <b>Report</b> button.</p> <p>In the <b>Compare/Merge</b> dialog box, enables the <b>Cancel</b> and <b>Help</b> buttons.</p> <p>In the <b>Potential Members</b> table, enables all functions in the right-click menu.</p> <p>In the <b>Zones</b> table, enables the <b>Port Label</b>, <b>Search</b>, and <b>Properties</b> (not editable) functions in the right-click menu.</p> <p>In the <b>Zone Configs</b> table, enables the <b>Properties</b> (not editable) function in the right-click menu.</p> | <p>Enables all functions on the <b>Zoning</b> dialog box.</p>                                                                                              |
| <p>Zone Set Edit Limits</p>                                                                                                                                                                                                                                                                                                       | <p>Allows you to set the number of zoning edit operations that can be performed on a fabric zone database before activating a zone configuration.</p>                     | <p>Disables the <b>Zoning &gt; Set Edit Limits</b> command from the <b>Configure</b> menu.</p>                                                                                                                                                                                                                                                    | <p>Enables the <b>Zoning &gt; Set Edit Limits</b> command from the <b>Configure</b> menu.</p> <p>Disables all commands and functions on the dialog box except the <b>Close</b> and <b>Help</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p>Enables the <b>Zoning &gt; Set Edit Limits</b> command from the <b>Configure</b> menu.</p> <p>Enables all commands and functions on the dialog box.</p> |

## About Roles and Access Levels

The Management application provides seven pre-configured roles (System Administrator, Security Administrator, Zone Administrator, Operator, Security Officer, Network Administrator, and Host Administrator); however, System Administrators can also create roles manually. Refer to [“Creating a user role”](#) on page 355 for instructions. The System Administrator is the only pre-configured role with Read and Write access to all features. Roles are automatically assigned to all resource groups.

**TABLE 36** Features and User Groups Access Levels

| Feature                            | Roles with Read/Write Access                                   | Roles with Read-Only Access                                            |
|------------------------------------|----------------------------------------------------------------|------------------------------------------------------------------------|
| Active Session Management          | System Administrator, Security Officer                         | Operator                                                               |
| Add/Delete Properties              | System Administrator, Host Administrator                       | Operator                                                               |
| Backup                             | System Administrator, Operator                                 |                                                                        |
| Call Home Event Notification Setup | System Administrator, Operator                                 |                                                                        |
| CEE Management                     | System Administrator, Network Administrator                    | Security Administrator, Security Officer                               |
| Configuration Management           | System Administrator                                           | Operator                                                               |
| Diagnose and Troubleshooting       | System Administrator                                           | Operator                                                               |
| Discovery Setup                    | System Administrator, Host Administrator                       | Operator                                                               |
| E-mail Event Notification Setup    | System Administrator, Operator                                 |                                                                        |
| Event Management                   | System Administrator                                           | Operator                                                               |
| Fabric Binding                     | System Administrator, Security Administrator, Security Officer | Operator                                                               |
| Fabric Tracking                    | System Administrator                                           | Operator                                                               |
| Fault Management                   | System Administrator                                           | Operator                                                               |
| FCIP Management                    | System Administrator                                           | Operator                                                               |
| FCoE Management                    | System Administrator, Network Administrator                    | Security Administrator, Zone Administrator, Security Officer, Operator |
| FICON Management                   | System Administrator                                           | Operator                                                               |
| Firmware Management                | System Administrator                                           | Operator                                                               |
| High Integrity Fabric              | System Administrator, Security Administrator, Security Officer | Operator                                                               |
| Host Management                    | System Administrator, Security Officer, Host Administrator     | Operator                                                               |
| License Update                     | System Administrator                                           | Operator                                                               |
| Logical Switch Configuration       | System Administrator                                           |                                                                        |
| LSAN Zoning                        | System Administrator, Zone Administrator                       | Operator                                                               |
| Map Port to Storage                | System Administrator                                           | Operator                                                               |
| Performance                        | System Administrator, Host Administrator                       | Operator                                                               |

**TABLE 36** Features and User Groups Access Levels (Continued)

| Feature                           | Roles with Read/Write Access                                                                                                            | Roles with Read-Only Access  |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Port Fencing                      | System Administrator                                                                                                                    | Operator                     |
| Product Administration            | System Administrator                                                                                                                    |                              |
| Product Maintenance               | System Administrator                                                                                                                    |                              |
| Product Operation                 | System Administrator, Operator                                                                                                          |                              |
| Properties Edit                   | System Administrator, Host Administrator                                                                                                | Operator                     |
| Report                            | System Administrator                                                                                                                    | Operator                     |
| Routing Configuration             | System Administrator                                                                                                                    | Operator                     |
| Security                          | System Administrator, Security Administrator, Security Officer, Host Administrator                                                      | Operator                     |
| Servers                           | System Administrator, Host Administrator                                                                                                | Operator                     |
| Setup Tools                       | System Administrator                                                                                                                    | Operator                     |
| SMIA Operations                   | System Administrator                                                                                                                    | Operator                     |
| Software Configuration Properties | System Administrator                                                                                                                    | Operator                     |
| Storage Encryption Configuration  | System Administrator, Security Administrator                                                                                            | Operator                     |
| Storage Encryption Key Operations | System Administrator, Security Administrator, Security Officer                                                                          |                              |
| Storage Encryption Security       | System Administrator, Security Administrator                                                                                            | Operator                     |
| Technical Support Data Collection | System Administrator                                                                                                                    | Operator                     |
| User Management                   | System Administrator, Security Officer                                                                                                  | Operator                     |
| View Management                   | System Administrator, Security Administrator, Zone Administrator, Network Administrator, Security Officer, Operator, Host Administrator |                              |
| Zoning Activation                 | System Administrator, Zone Administrator                                                                                                | Operator                     |
| Zoning Offline                    | System Administrator, Zone Administrator                                                                                                | Operator                     |
| Zoning Online                     | System Administrator, Zone Administrator                                                                                                | Operator                     |
| Zoning Set Edit Limits            | System Administrator                                                                                                                    | Zone Administrator, Operator |

# Sybase and Derby Database Fields

---

## In this appendix

|                                   |     |
|-----------------------------------|-----|
| • Advanced Call Home .....        | 720 |
| • Capability .....                | 721 |
| • Client_view .....               | 722 |
| • Collector .....                 | 725 |
| • Config .....                    | 728 |
| • Connected end devices .....     | 730 |
| • Device .....                    | 731 |
| • EE- Monitor .....               | 738 |
| • Event/FM .....                  | 740 |
| • Fabric .....                    | 746 |
| • FC Port Stats .....             | 749 |
| • FCIP .....                      | 752 |
| • FCIP Tunnel Stats .....         | 755 |
| • GigE Port Stats .....           | 757 |
| • ISL .....                       | 759 |
| • License .....                   | 762 |
| • Encryption Device .....         | 763 |
| • Encryption Container .....      | 769 |
| • Meta SAN .....                  | 774 |
| • Network .....                   | 776 |
| • Others .....                    | 777 |
| • Port Fencing .....              | 778 |
| • Quartz .....                    | 779 |
| • Reports .....                   | 782 |
| • Role Based Access Control ..... | 782 |
| • SNMP .....                      | 785 |
| • Stats .....                     | 788 |
| • Switch .....                    | 790 |
| • Switch details .....            | 795 |
| • Switch port .....               | 800 |
| • Threshold .....                 | 807 |
| • User Interface .....            | 808 |

- [Zoning 1](#) ..... 809
- [Zoning 2](#) ..... 811

## Database tables and fields

### Advanced Call Home

#### NOTE

The primary keys are marked by an asterisk (\*).

**TABLE 37** ACH\_CALL\_CENTER

| Field | Definition               | Format  | Size |
|-------|--------------------------|---------|------|
| ID *  |                          | int     |      |
| NAME  | Name of the Call Center. | varchar | 256  |

**TABLE 38** ACH\_CALL\_CENTRE\_CONFIG

| Field            | Definition                                                            | Format  | Size |
|------------------|-----------------------------------------------------------------------|---------|------|
| KEY_ *           | Key to identify the specific configuration of the Call Center.        | varchar | 256  |
| CALL_CENTER_ID * | ID of the Call Center.                                                | int     |      |
| VALUE            | Value of specific configuration identified by Key of the Call Center. | varchar | 256  |

**TABLE 39** ACH\_INFO

| Field          | Definition                                                                                    | Format   | Size |
|----------------|-----------------------------------------------------------------------------------------------|----------|------|
| ID*            |                                                                                               | int      |      |
| SWITCH_WWN     | WWN of the switch.                                                                            | varchar  | 23   |
| FILTER_ID      | If an event filter is assigned to the switch - the filter ID if no filter is assigned - null. | int      |      |
| CALL_CENTER_ID | ID of the call center to which the switch is assigned.                                        | int      |      |
| SUPPORT_SAVE   | 1 = Support save is enabled for the switch.<br>0 = Support save is disabled for the switch.   | smallint |      |

**TABLE 40** ACH\_FILTER

| Field       | Definition                       | Format  | Size |
|-------------|----------------------------------|---------|------|
| ID*         |                                  | int     |      |
| NAME        | Name of the event filter.        | varchar | 256  |
| DESCRIPTION | Description of the event filter. | varchar | 256  |

**TABLE 41** ACH\_EVENT\_FILTER\_MAP

| Field       | Definition                                             | Format | Size |
|-------------|--------------------------------------------------------|--------|------|
| FILTER_ID * | ID of the event filter.                                | int    |      |
| EVENT_ID *  | Event ID which needs to be associated with the filter. | int    |      |

**TABLE 42** ACH\_EVENT

| Field       | Definition                | Format  | Size |
|-------------|---------------------------|---------|------|
| ID *        |                           | int     |      |
| REASON_CODE | Reason code of the event. | varchar | 256  |
| FRU_CODE    | FRU code of the event.    | varchar | 256  |
| DESCRIPTION | Description of the event. | varchar | 256  |
| SEVERITY    | Severity of the event.    | int     |      |
| TYPE        | Type of the event.        | varchar | 256  |

## Capability

**TABLE 43** CAPABILITY\_

| Field       | Definition                                          | Format  | Size |
|-------------|-----------------------------------------------------|---------|------|
| NAME *      | Name of the capability.                             | varchar | 256  |
| DESCRIPTION | Optional detailed description about the capability. | varchar | 512  |

**TABLE 44** CARD\_CAPABILITY

| Field         | Definition                                   | Format  | Size |
|---------------|----------------------------------------------|---------|------|
| CARD_ID *     | DB ID of the card.                           | int     |      |
| CAPABILITY_ * | Name of the capability detected on the card. | varchar | 256  |
| ENABLED       | 1 = the capability is enabled on the card.   | int     |      |

**TABLE 45** VIRTUAL\_SWITCH\_CAPABILITY

| Field               | Definition                                           | Format  | Size |
|---------------------|------------------------------------------------------|---------|------|
| VIRTUAL-SWITCH_ID * | DB ID of virtual switch.                             | int     |      |
| CAPABILITY_ *       | Name of capability detected on virtual switch.       | varchar | 256  |
| ENABLED             | 1 = the capability is enabled on the virtual switch. | int     |      |

**TABLE 46** CARD

| Field                | Definition                                                                                                          | Format   | Size |
|----------------------|---------------------------------------------------------------------------------------------------------------------|----------|------|
| ID *                 |                                                                                                                     | int      |      |
| CORE_SWITCH_ID *     | Core switch DB ID.                                                                                                  | int      |      |
| SLOT_NUMBER          | The number of the physical slot in the chassis where the blade is plugged in. For fixed blades, SlotNumber is zero. | smallint |      |
| TYPE                 | ID of the blade to identify the type.                                                                               | smallint |      |
| EQUIPEMNT_TYPE       | The type of the blade. It is either SW BLADE or CP BLADE.                                                           | varchar  | 16   |
| STATE                | State of the blade, such as ENABLED or DISABLED.                                                                    | varchar  | 32   |
| POWER_STATE          | State of power supply to the blade.                                                                                 | varchar  | 16   |
| ATTN_STATE           |                                                                                                                     | varchar  | 32   |
| SERIAL_NUMBER        | Factory serial number of the blade.                                                                                 | varchar  | 32   |
| PART_NUMBER          | The part number assigned by the organization responsible for producing or manufacturing the blade.                  | varchar  | 32   |
| TRUNKING_SUPPORTED   | 1 = trunking is supported on this blade.                                                                            | smallint |      |
| FICON_DISABLED       | 1 = FICON is disabled on this blade.                                                                                | smallint |      |
| IP_ADDRESS           | IP address of first Ethernet management port for a given slot with intelligent blade.                               | char     | 64   |
| SUBNET_MASK          | Mask of first Ethernet man.agement port for a given slot with intelligent blade.                                    | varchar  | 64   |
| DEFAULT_GATEWAY      | Gateway IP address Ethernet management for a given slot with intelligent blade.                                     | varchar  | 64   |
| PRIMARY_FW_VERSION   | Primary firmware version of applications on this blade. Applicable only for AP_BLADE.                               | varchar  | 48   |
| SECONDARY_FW_VERSION | Secondary firmware version applications on this blade. Applicable only for AP_BLADE.                                | varchar  | 48   |

**TABLE 47** CORE\_SWITCH\_CAPABILITY

| Field            | Definition                                          | Format  | Size |
|------------------|-----------------------------------------------------|---------|------|
| CORE_SWITCH_ID * | DB ID.                                              | int     |      |
| CAPABILITY_ *    | Name of the capability detected on the core switch. | varchar | 256  |
| ENABLED          | 1 = the capability is enabled on the core switch.   | int     |      |

## Client\_view

**TABLE 48** USER\_

| Field       | Definition        | Format  | Size |
|-------------|-------------------|---------|------|
| NAME *      | User name.        | varchar | 128  |
| DESCRIPTION | User description. | varchar | 512  |

**TABLE 48** USER\_ (Continued)

| Field                | Definition                    | Format   | Size |
|----------------------|-------------------------------|----------|------|
| PASSWORD             | User password.                | varchar  | 128  |
| EMAIL                | User e-mail ID.               | varchar  | 1024 |
| NOTIFICATION_ENABLED | Flag for e-mail notification. | smallint |      |

**TABLE 49** USER\_PREFERENCE

| Field       | Definition                                                                        | Format       | Size |
|-------------|-----------------------------------------------------------------------------------|--------------|------|
| USER_NAME * | User name whose preferences are saved. It corresponds to user_name in USER_table. | varchar      | 128  |
| CATEGORY *  | The name for a set of related preferences.                                        | varchar      | 128  |
| CONTENT     | The set of preferences saved as name-value pairs.                                 | long varchar |      |

**TABLE 50** CLIENT\_VIEW

| Field       | Definition                            | Format  | Size |
|-------------|---------------------------------------|---------|------|
| ID *        |                                       | int     |      |
| USER_NAME   | The Management application user name. | varchar | 128  |
| NAME        | Client view name.                     | varchar | 255  |
| DESCRIPTION | Client View description.              | varchar | 255  |

**TABLE 51** CLIENT\_VIEW\_COLUMN

| Field           | Definition                                                                                                                    | Format    | Size |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| ID *            |                                                                                                                               | int       |      |
| NAME            | Column name.                                                                                                                  | varchar   | 255  |
| ENTITY_CATEGORY | Either "fabric" or "product (switch or device)" or "port"; or combination of these 3 basic categories.                        | varchar   | 128  |
| COLUMN_INDEX    | 0 = Predefined column.<br>1 = First user-defined column.<br>2 = Second user-defined column.<br>3 = Third user-defined column. | small int |      |
| DESCRIPTION     | Column description, typically populated for user-defined columns.                                                             | varchar   | 255  |
| ICON_ID         | Not used.                                                                                                                     | int       |      |
| VISIBLE         | 1 = all predefined / fixed columns.<br>0 = user-defined columns.                                                              | smallint  |      |
| EDITABLE        | 1 = column is editable.<br>0 = column is not editable.                                                                        | smallint  |      |

**TABLE 52** CLIENT\_VIEW\_MEMBER

| Field            | Definition                        | Format | Size |
|------------------|-----------------------------------|--------|------|
| CLIENT_VIEW_ID * | Foreign key to CLIENT_VIEW table. | int    |      |
| FABRIC_ID *      | Foreign key to FABRIC table.      | int    |      |

**TABLE 53** FABRIC

| Field                | Definition                                                                         | Format    | Size |
|----------------------|------------------------------------------------------------------------------------|-----------|------|
| ID *                 |                                                                                    | int       |      |
| SAN_ID               | Foreign key to SAN table; usually 1 since there is only one SAN.                   | int       |      |
| SEED_SWITCH_WWN      | WWN of the virtual switch used as seed switch to discover the fabric.              | char      | 23   |
| NAME                 | User-assigned fabric name.                                                         | varchar   | 256  |
| CONTACT              | User-assigned "contact" for the fabric.                                            | varchar   | 256  |
| LOCATION             | User-assigned "location" for the fabric.                                           | varchar   | 256  |
| DESCRIPTION          | User-assigned fabric description.                                                  | varchar   | 256  |
| TYPE                 | Type of fabric:<br>0 = legacy fabric.<br>1 = base fabric.<br>2 = logical fabric.   | smallint  |      |
| SECURE               | 1 = it is a secured fabric.                                                        | smallint  |      |
| AD_ENVIRONMENT       | 1 = there are user-defined ADs in this fabric.                                     | smallint  |      |
| MANAGED              | 1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric | smallint  |      |
| MANAGEMENT_STATE     | Bit map to indicate various management indications for the fabric.                 | smallint  |      |
| TRACK_CHANGES        | 1 = changes (member switches, ISL and devices) in the fabric are tracked.          | smallint  |      |
| STATS_COLLECTION     | 1 = statistics collection is enabled on the fabric.                                | smallint  |      |
| CREATION_TIME        | When the fabric record is inserted, i.e., created.                                 | timestamp |      |
| LAST_FABRIC_CHANGED  | Time when fabric last changed.                                                     | timestamp |      |
| LAST_SCAN_TIME       |                                                                                    | timestamp |      |
| LAST_UPDATE_TIME     | Time when fabric was last updated.                                                 | timestamp |      |
| ACTIVE_ZONESET_NAME  | Name of the zone configuration which is effective / active in that fabric.         | varchar   | 256  |
| USER_DEFINED_VALUE_1 | User-defined custom value.                                                         | varchar   | 256  |
| USER_DEFINED_VALUE_2 | User-defined custom value.                                                         | varchar   | 256  |
| USER_DEFINED_VALUE_3 | User-defined custom value.                                                         | varchar   | 256  |

## Collector

**TABLE 54** FABRIC\_CHECKSUM

| Field          | Definition                                       | Format  | Size |
|----------------|--------------------------------------------------|---------|------|
| FABRIC_ID *    | Fabric ID, foreign key to the FABRIC table.      | int     |      |
| CHECKSUM_KEY * | Type of checksum, e.g. device data or zone data. | varchar | 32   |
| CHECKSUM       | Actual checksum value.                           | varchar | 16   |

**TABLE 55** FABRIC\_COLLECTION

| Field                     | Definition                                                                                                                                             | Format    | Size |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| FABRIC_ID *               | Fabric ID, foreign key to the FABRIC table.                                                                                                            | int       |      |
| COLLECTOR_NAME *          | Name of the collector, e.g., NameServerInfoCollector, TopologyCollector, ZoneInfoCollector, ActiveZoneInfoCollector.                                   | varchar   | 256  |
| SEED_SWITCH_IP            | IP address of the switch which serves as the seed switch. This is the switch from which above mentioned fabric level collectors get their information. | varchar   | 128  |
| LAST_SEED_SW_MODIFICATION | Timestamp of the seed switch, when the particular HTML page was changed last. Note that this is not when the last time collection was done.            | timestamp |      |

**TABLE 56** COLLECTOR

| Field       | Definition                                                      | Format  | Size |
|-------------|-----------------------------------------------------------------|---------|------|
| NAME *      | Name of the collector registered with the collection framework. | varchar | 256  |
| CLASS_NAME  | Java class name which serves as the collector.                  | varchar | 256  |
| DESCRIPTION | Collector description, usually not used.                        | varchar | 512  |

**TABLE 57** FABRIC

| Field           | Definition                                                            | Format   | Size |
|-----------------|-----------------------------------------------------------------------|----------|------|
| ID *            |                                                                       | int      |      |
| SAN_ID          | Foreign key to SAN table; usually 1 since there is only one SAN.      | int      |      |
| SEED_SWITCH_WWN | WWN of the virtual switch used as seed switch to discover the fabric. | char     | 23   |
| NAME            | User-assigned fabric name.                                            | varchar  | 256  |
| CONTACT         | User-assigned "contact" for the fabric.                               | varchar  | 256  |
| LOCATION        | User-assigned "location" for the fabric.                              | varchar  | 256  |
| DESCRIPTION     | User-assigned fabric description.                                     | varchar  | 256  |
| TYPE            | Type of fabric (0: legacy fabric, 1: base fabric, 2: logical fabric). | smallint |      |
| SECURE          | 1 = it is a secured fabric.                                           | smallint |      |

**TABLE 57** FABRIC (Continued)

| Field                | Definition                                                                          | Format    | Size |
|----------------------|-------------------------------------------------------------------------------------|-----------|------|
| AD_ENVIRONMENT       | 1 = there are user-defined ADs in this fabric.                                      | smallint  |      |
| MANAGED              | 1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric. | smallint  |      |
| MANAGEMENT_STATE     | Bit map to indicate various management indications for the fabric.                  | smallint  |      |
| TRACK_CHANGES        | 1 = changes (member switches, ISL and devices) in the fabric are tracked.           | smallint  |      |
| STATS_COLLECTION     | 1 = statistics collection is enabled on the fabric.                                 | smallint  |      |
| CREATION_TIME        | When the fabric record is inserted, i.e., created.                                  | timestamp |      |
| LAST_FABRIC_CHANGED  | Time when fabric last changed.                                                      | timestamp |      |
| LAST_SCAN_TIME       |                                                                                     | timestamp |      |
| LAST_UPDATE_TIME     | Time when fabric was last updated.                                                  | timestamp |      |
| ACTIVE_ZONESET_NAME  | Name of the zone configuration which is effective / active in that fabric.          | varchar   | 256  |
| USER_DEFINED_VALUE_1 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_2 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_3 | User-defined custom value.                                                          | varchar   | 256  |

**TABLE 58** COLLECTOR\_END\_TIMESTAMP

| Field                 | Definition                                                                                                         | Format    | Size |
|-----------------------|--------------------------------------------------------------------------------------------------------------------|-----------|------|
| COLLECTOR_SOURCE *    | Internal key for switches and fabrics for which collection is undertaken.                                          | varchar   | 256  |
| COLLECTOR_NAME *      | Collection name, Java class used to collect specific fabric or switch information.                                 | varchar   | 256  |
| TIMESTAMP_            | When the last successful collection is done.                                                                       | timestamp |      |
| LAST_COLLECTED_STATUS | Status of the last collection, successful or not. 200 is for successful. Values are standard HTTP protocol values. | smallint  |      |

**TABLE 59** VIRTUAL\_SWITCH\_COLLECTION

| Field                        | Definition                    | Format    | Size |
|------------------------------|-------------------------------|-----------|------|
| VIRTUAL_SWITCH_ID *          | DB ID of virtual switch.      | int       |      |
| COLLECTOR_NAME *             | Collector name.               | varchar   | 256  |
| LAST_VIRTUAL_SW_MODIFICATION | Last modified time on switch. | timestamp |      |

**TABLE 60** VIRTUAL\_SWITCH\_CHECKSUM

| Field               | Definition               | Format  | Size |
|---------------------|--------------------------|---------|------|
| VIRTUAL_SWITCH_ID * | DB ID of virtual switch. | int     |      |
| CHECKSUM_KEY *      | Checksum key.            | varchar | 32   |
| CHECKSUM            | Checksum value.          | varchar | 16   |

**TABLE 61** CORE\_SWITCH\_CHECKSUM

| Field            | Definition      | Format  | Size |
|------------------|-----------------|---------|------|
| CORE_SWITCH_ID * | DB ID.          | int     |      |
| CHECKSUM_KEY *   | Checksum type.  | varchar | 32   |
| CHECKSUM         | Checksum value. | varchar | 16   |

**TABLE 62** CORE\_SWITCH\_COLLECTION

| Field                         | Definition                          | Format    | Size |
|-------------------------------|-------------------------------------|-----------|------|
| CORE_SWITCH_ID *              | Core switch ID.                     | int       |      |
| COLLECTION_NAME *             | Collector name.                     | varchar   | 256  |
| LAST_CORE_SW_<br>MODIFICATION | Last core switch modification time. | timestamp |      |

**TABLE 63** SECURITY\_POLICY

| Field                          | Definition                                                                                                                                   | Format   | Size |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| VIRTUAL_SWITCH_ID *            | DB ID of virtual_switch.                                                                                                                     | int      |      |
| POLICY_NUMBER*                 | IPSec Policy Number. The number can range from 1 to 32.                                                                                      | smallint |      |
| POLICY_TYPE*                   | Type of the Policy. The possible values are IKE or IPSec                                                                                     | smallint |      |
| ENCRYPTION_ALGORITHM           | Encryption Algorithm for the policy. The following are the possible Encryption: NONE, DES, 3DES, AES-128, AES-256, AES-CM-128 or AES-CM-256. | varchar  | 32   |
| AUTHENTICATION_ALGORITHM       | Authentication Algorithm for the policy:<br>NONE<br>SHA-1<br>MD5<br>AES-XCBC                                                                 | varchar  | 32   |
| PERFECT_FORWARD_POLICY_ENABLED | Perfect Forward Secrecy for the policy. The possible values are 0 or 1.                                                                      | smallint |      |
| DIFFIE_HELLMAN_GROUP           | Diffie-Hellman Group used in PFS negotiation.                                                                                                | smallint |      |
| SECURITY_ASSOC_LIFE            | Association lifetime in seconds.                                                                                                             | double   |      |
| SECURITY_ASSOC_LIFE_IN_MB      | Security association lifetime in megabytes.                                                                                                  | double   |      |

## Config

**TABLE 64** FIRMWARE\_SWITCH\_DETAIL

| Field           | Definition                                    | Format   | Size |
|-----------------|-----------------------------------------------|----------|------|
| FIRMWARE_ID*    | ID for the firmware file.                     | int      |      |
| SWITCH_TYPE*    | Switch type that supports this firmware file. | smallint |      |
| REBOOT_REQUIRED | Reboot required flag for the switch type.     | smallint |      |
| NUMFILES        | Number of files in the firmware.              | int      |      |

**TABLE 65** FIRMWARE\_FILE\_DETAIL

| Field         | Definition                                   | Format   | Size |
|---------------|----------------------------------------------|----------|------|
| ID*           |                                              | int      |      |
| FIRMWARE_NAME | Name of the firmware file.                   | varchar  | 64   |
| MAJOR_VERSION | Major version bit from the firmware version. | smallint |      |
| MINOR_VERSION | Minor version bit from the firmware version. | smallint |      |
| MAINTENANCE   | Maintenance bit from the firmware version.   | smallint |      |
| PATCH         | Patch bit from the firmware version.         | varchar  | 64   |
| PHASE         | Phase bit from the firmware version.         | varchar  | 64   |

**TABLE 65** FIRMWARE\_FILE\_DETAIL (Continued)

| Field                    | Definition                                                                            | Format    | Size |
|--------------------------|---------------------------------------------------------------------------------------|-----------|------|
| RELEASE_DATE             | Release date of the firmware file.                                                    | timestamp |      |
| IMPORTED_DATE            | Imported date of the file to the Management application.                              | timestamp |      |
| FIRMWARE_FILE_SIZE       | Firmware file size.                                                                   | int       |      |
| FIRMWARE_LOCATION        | Firmware file location in the Management application repository.                      | varchar   | 1024 |
| RELEASE_NOTES_LOCATION   | Release notes file location in the Management application repository.                 | varchar   | 1024 |
| FIRMWARE_REPOSITORY_TYPE | Repository type to identify the FTP server:<br>0 = internal FTP.<br>1 = external FTP. | smallint  |      |

**TABLE 66** SWITCH\_PLATFORM

| Field            | Definition                         | Format   | Size |
|------------------|------------------------------------|----------|------|
| SWITCH_TYPE*     | Switch type.                       | smallint |      |
| DESCRIPTION      | Description of the switch type.    | varchar  | 256  |
| SPEED            | Switch maximum speed.              | smallint |      |
| MULTI_CP_CAPABLE | Switch is multi-CP capable or not. | smallint |      |

**TABLE 67** FTP\_SERVER

| Field          | Definition                                                                        | Format   | Size |
|----------------|-----------------------------------------------------------------------------------|----------|------|
| ID*            |                                                                                   | int      |      |
| TYPE           | Type indicates the FTP is internal or external.<br>0 = internal.<br>1 = external. | smallint |      |
| IP             | FTP server IP address.                                                            | varchar  | 64   |
| USER_NAME      | FTP server user name.                                                             | varchar  | 64   |
| PASSWORD       | FTP server user password.                                                         | varchar  | 64   |
| ROOT_DIRECTORY | FTP server root directory location.                                               | varchar  | 1024 |
| PORT           | Port on which FTP server is configured.                                           | int      |      |

**TABLE 68** SWITCH\_TYPE\_FIRMWARE\_VERSION

| Field            | Definition                          | Format   | Size |
|------------------|-------------------------------------|----------|------|
| SWITCH_TYPE*     | Switch type.                        | smallint |      |
| MIN_FOS_VERSION* | Supported minimum firmware version. | varchar  | 64   |
| MAX_FOS_VERSION  | Supported maximum firmware version. | varchar  | 64   |

**TABLE 69** SWITCH\_CONFIG

| Field            | Definition                                                                                        | Format      | Size |
|------------------|---------------------------------------------------------------------------------------------------|-------------|------|
| NAME             | Name of the switch configurations uploaded from the switch either on demand or through scheduler. | int         |      |
| ID*              |                                                                                                   | varchar     | 64   |
| SWITCH_ID        | ID of the switch from which the configuration has been uploaded.                                  | int         |      |
| BACKUP_DATE_TIME | The date/time stamp at which the configuration has been uploaded.                                 | timestamp   |      |
| CONFIG_DATA      | The actual switch configuration data.                                                             | longvarchar |      |
| KEEP_COPY        | The column value (1) helps to preserve the configuration even after the expiration of its age.    | smallint    |      |
| CREATED_BY       | The column value helps to figure out who triggered the configuration upload operation.            | varchar     | 64   |

## Connected end devices

**TABLE 70** CED\_APPLICATION

| Field     | Definition                                                                                | Format  | Size |
|-----------|-------------------------------------------------------------------------------------------|---------|------|
| ID*       |                                                                                           | int     |      |
| NAME      | Name of the application. Application represents a collection of active zones in a fabric. | varchar | 24   |
| FABRIC_ID | ID of the fabric for which the application is created.                                    | int     |      |

**TABLE 71** CED\_APPLICATION\_MEMBER

| Field           | Definition                                                                  | Format | Size |
|-----------------|-----------------------------------------------------------------------------|--------|------|
| APPLICATION_ID* | Auto-generated DB CED_Application table ID.                                 | int    |      |
| ZONE_ID*        | Auto-generated DB Zone table ID which joins as a member of the application. | int    |      |

**TABLE 72** CED\_USER\_PREFERENCE

| Field          | Definition                                                                              | Format  | Size |
|----------------|-----------------------------------------------------------------------------------------|---------|------|
| USER_NAME*     | User Name carried from _USER table.                                                     | varchar | 128  |
| FABRIC_ID*     | Fabric ID carried from Fabric table.                                                    | int     |      |
| APPLICATION_ID | CED application ID representing the group of end devices to be displayed in the fabric. | int     |      |

## Device

**TABLE 73** DEVICE\_PORT

| Field            | Definition                                                                                                                                                                                                                                                                                                                                                                   | Format    | Size |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| ID*              |                                                                                                                                                                                                                                                                                                                                                                              | int       |      |
| NODE_ID          | DB ID of the device node to which this port belongs.                                                                                                                                                                                                                                                                                                                         | int       |      |
| DOMAIN_ID        | Domain ID of the switch to which this device port is attached.                                                                                                                                                                                                                                                                                                               | int       |      |
| WWN              | Device port WWN.                                                                                                                                                                                                                                                                                                                                                             | char      | 23   |
| SWITCH_PORT_WWN  | WWN of the switch port to which this device port is attached.                                                                                                                                                                                                                                                                                                                | char      | 23   |
| NUMBER           | Switch port number to which this device is attached.                                                                                                                                                                                                                                                                                                                         | smallint  |      |
| PORT_ID          | Device port ID.                                                                                                                                                                                                                                                                                                                                                              | varchar   | 6    |
| TYPE             | Device port type, such as N or NL.                                                                                                                                                                                                                                                                                                                                           | varchar   | 32   |
| SYMBOLIC_NAME    | Device port symbolic name.                                                                                                                                                                                                                                                                                                                                                   | varchar   | 256  |
| FC4_TYPE         | FC payload protocol.                                                                                                                                                                                                                                                                                                                                                         | varchar   | 16   |
| COS              | FC class of service.                                                                                                                                                                                                                                                                                                                                                         | varchar   | 16   |
| IP_PORT          |                                                                                                                                                                                                                                                                                                                                                                              | varchar   | 63   |
| HARDWARE_ADDRESS |                                                                                                                                                                                                                                                                                                                                                                              | varchar   | 6    |
| TRUSTED          | 1 if found at discovery time or user has entrusted this device port explicitly.                                                                                                                                                                                                                                                                                              | smallint  |      |
| CREATION_TIME    | When the device port was discovered, i.e., created in the DB.                                                                                                                                                                                                                                                                                                                | timestamp |      |
| MISSING          | 1 if that device port is missing from the fabric.                                                                                                                                                                                                                                                                                                                            | smallint  |      |
| MISSING_TIME     | Time when it misses.                                                                                                                                                                                                                                                                                                                                                         | timestamp |      |
| NPV_PHYSICAL     | Update NPV device type on this given device port. The value "npvPhysical" on the device port will be 1 when the device port has reference to a device node of DEVICE_TYPE value 0 i.e. physical. It points to a switch port to which at least one other device port points; and that other pointing device port has reference to a device node of DEVICE_TYPE value 2 (NPV). | smallint  |      |

**TABLE 74** FICON\_DEVICE\_PORT

| Field              | Definition                                                             | Format  | Size |
|--------------------|------------------------------------------------------------------------|---------|------|
| DEVICE_PORT_ID*    | Value for the device port to which these FICON properties are applied. | int     |      |
| TYPE_NUMBER        |                                                                        | varchar | 16   |
| MODEL_NUMBER       | Ficon device model number, such as S18.                                | varchar | 64   |
| MANUFACTURER       | Manufacturer of the device, typically IBM.                             | varchar | 64   |
| MANUFACTURER_PLANT | Plant number where the device is manufactured.                         | varchar | 64   |
| SEQUENCE_NUMBER    | Device sequence number.                                                | varchar | 32   |

**TABLE 74** FICON\_DEVICE\_PORT (Continued)

| Field  | Definition                                              | Format  | Size |
|--------|---------------------------------------------------------|---------|------|
| TAG    | FICON device property, e.g., 809a or 809b.              | varchar | 16   |
| FLAG   | FICON device property, e.g., 0x10 (hex).                | varchar | 8    |
| PARAMS | FICON device property string, e.g., Valid channel port. | varchar | 16   |

**TABLE 75** DEVICE\_NODE

| Field          | Definition                                                                                                                                                                                         | Format    | Size |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| ID*            |                                                                                                                                                                                                    | int       |      |
| FABRIC_ID      | Fabric DB ID to which this device node belongs.                                                                                                                                                    | int       |      |
| WWN            | Device node WWN.                                                                                                                                                                                   | char      | 23   |
| TYPE           | Initiator or target or both or unknown.                                                                                                                                                            | varchar   | 32   |
| DEVICE_TYPE    | 0 = physical<br>1 = virtual<br>2 = NPV<br>3 = iSCSI<br>4 = both physical & virtual                                                                                                                 | smallint  |      |
| SYMBOLIC_NAME  | Device node symbolic name.                                                                                                                                                                         | varchar   | 256  |
| FCMI_HOST_NAME | Device node FDMI host name.                                                                                                                                                                        | varchar   | 128  |
| VENDOR         | Device node vendor.                                                                                                                                                                                | varchar   | 64   |
| CAPABILITY_    |                                                                                                                                                                                                    | varchar   | 16   |
| TRUSTED        | 1 = the node is trusted for "fabric tracking."                                                                                                                                                     | smallint  |      |
| CREATION_TIME  | Timestamp when the record is created by the Management application server.                                                                                                                         | timestamp |      |
| MISSING        | 1 = the device node is missing from the fabric.                                                                                                                                                    | smallint  |      |
| MISSING_TIME   | Time when the device node missed.                                                                                                                                                                  | timestamp |      |
| PROXY_DEVICE   | One of the device ports of this device node has translated domain. That device port is set as the Proxy Device and this Device Node is treated as virtual by assigning a value of 1 to this field. | smallint  |      |
| AG             | 1 = the device node is actually an AG connected to a switch in the fabric.                                                                                                                         | smallint  |      |

**TABLE 76** DEVICE\_ENCLOSURE\_MEMBER

| Field            | Definition                                                                         | Format | Size |
|------------------|------------------------------------------------------------------------------------|--------|------|
| ENCLOSURE_ID*    | DEVICE_ENCLOSURE table ID.                                                         | int    |      |
| DEVICE_PORT_WWN* | Comment on column DEVICE_ENCLOSURE_MEMBER.DEVICE_PORT_WWN is 'WWN Of Device Port'. | char   | 23   |
| DEVICE_PORT_ID   | Device_Port table ID.                                                              | int    |      |

**TABLE 77** DEVICE\_ENCLOSURE

| Field               | Definition                                                                                  | Format  | Size |
|---------------------|---------------------------------------------------------------------------------------------|---------|------|
| ID*                 |                                                                                             | int     |      |
| FABRIC_ID           | ID of the fabric to which the device enclosure belongs.                                     | int     |      |
| NAME                | Name of the Device enclosure.                                                               | varchar | 256  |
| TYPE                | Type of Device enclosure - Storage Array/Server.                                            | varchar | 32   |
| ICON                | Type of Icon.                                                                               | int     |      |
| OS                  | Operating System.                                                                           | varchar | 256  |
| APPLICATIONS        | Application which created device enclosure.                                                 | varchar | 256  |
| DEPARTMENT          | Department using this device enclosure.                                                     | varchar | 256  |
| CONTACT             | Contact person details.                                                                     | varchar | 256  |
| LOCATION            | Location of physical setup.                                                                 | varchar | 256  |
| DESCRIPTION         | Description if any.                                                                         | varchar | 256  |
| COMMENT             | Comments if any.                                                                            | varchar | 256  |
| IP_ADDRESS          | IP Address if assigned by user.                                                             | varchar | 128  |
| VENDOR              | Vendor name.                                                                                | varchar | 256  |
| MODEL               | Device enclosure Model.                                                                     | varchar | 256  |
| SERIAL_NUMBER       | Serial Number given for the entity.                                                         | varchar | 256  |
| FIRMWARE            | Firmware running on the device which is not applicable for device enclosure logical entity. | varchar | 256  |
| USER_DEFINED_VALUE1 | User-defined custom value.                                                                  | varchar | 256  |
| USER_DEFINED_VALUE2 | User-defined custom value.                                                                  | varchar | 256  |
| USER_DEFINED_VALUE3 | User-defined custom value.                                                                  | varchar | 256  |

**TABLE 78** FABRIC

| Field           | Definition                                                                    | Format   | Size |
|-----------------|-------------------------------------------------------------------------------|----------|------|
| ID*             |                                                                               | int      |      |
| SAN_ID          | Foreign key to SAN table; usually 1 since there is only one SAN.              | int      |      |
| SEED_SWITCH_WWN | WWN of the virtual switch used as seed switch to discover the fabric.         | char     | 23   |
| NAME            | User-assigned fabric name.                                                    | varchar  | 256  |
| CONTACT         | User-assigned "contact" for the fabric.                                       | varchar  | 256  |
| LOCATION        | User-assigned "location" for the fabric.                                      | varchar  | 256  |
| DESCRIPTION     | User-assigned fabric description.                                             | varchar  | 256  |
| TYPE            | Type of fabric:<br>0 = legacy fabric<br>1 = base fabric<br>2 = logical fabric | smallint |      |

**TABLE 78** FABRIC (Continued)

| Field                | Definition                                                                          | Format    | Size |
|----------------------|-------------------------------------------------------------------------------------|-----------|------|
| SECURE               | 1 = it is secured fabric.                                                           | smallint  |      |
| AD_ENVIRONMENT       | 1 = there are user-defined ADs in this fabric.                                      | smallint  |      |
| MANAGED              | 1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric. | smallint  |      |
| MANAGEMENT_STATE     | Bit map to indicate various management indications for the fabric.                  | smallint  |      |
| TRACK_CHANGES        | 1 = changes (member switches, ISL and devices) in the fabric are tracked.           | smallint  |      |
| STATS_COLLECTION     | 1 = statistics collection is enabled on the fabric.                                 | smallint  |      |
| CREATION_TIME        | When the fabric record is inserted, i.e., created.                                  | timestamp |      |
| LAST_FABRIC_CHANGED  | Time when the fabric last changed.                                                  | timestamp |      |
| LAST_SCAN_TIME       |                                                                                     | timestamp |      |
| LAST_UPDATE_TIME     | Time when the fabric was last updated.                                              | timestamp |      |
| ACTIVE_ZONESET_NAME  | Name of the zone configuration which is effective / active in that fabric.          | varchar   | 256  |
| USER_DEFINED_VALUE_1 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_2 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_3 | User-defined custom value.                                                          | varchar   | 256  |

**TABLE 79** DEVICE\_PORT\_INFO

| Name             | Source                       |
|------------------|------------------------------|
| ID               | DEVICE_PORT.ID               |
| NODE ID          | DEVICE_PORT.NODE_ID          |
| DOMAIN ID        | DEVICE_PORT.DOMAIN_ID        |
| WWN              | DEVICE_PORT.WWN              |
| SWITCH PORT WWN  | DEVICE_PORT.SWITCH_PORT_WWN  |
| NUMBER           | DEVICE_PORT.NUMBER           |
| PORT ID          | DEVICE_PORT.PORT_ID          |
| TYPE             | DEVICE_PORT.TYPE             |
| SYMBOLIC NAME    | DEVICE_PORT.SYMBOLIC_NAME    |
| FC4 TYPE         | DEVICE_PORT.FC4_TYPE         |
| COS              | DEVICE_PORT.COS              |
| IP PORT          | DEVICE_PORT.IP_PORT          |
| HARDWARE ADDRESS | DEVICE_PORT.HARDWARE_ADDRESS |
| TRUSTED          | DEVICE_PORT.TRUSTED          |
| CREATION TIME    | DEVICE_PORT.CREATION_TIME    |
| MISSING          | DEVICE_PORT.MISSING          |

**TABLE 79**    DEVICE\_PORT\_INFO

| Name                | Source                                         |
|---------------------|------------------------------------------------|
| MISSING TIME        | DEVICE_PORT.MISSING_TIME,                      |
| NPV PHYSICAL        | DEVICE_PORT.NPV_PHYSICAL                       |
| TYPE NUMBER         | FICON_DEVICE_PORT.TYPE_NUMBER                  |
| MODEL NUMBER        | FICON_DEVICE_PORT.MODEL_NUMBER                 |
| MANUFACTURER        | FICON_DEVICE_PORT.MANUFACTURER                 |
| MANUFACTURER PLANT  | FICON_DEVICE_PORT.MANUFACTURER_PLANT           |
| SEQUENCE NUMBER     | FICON_DEVICE_PORT.SEQUENCE_NUMBER              |
| TAG                 | FICON_DEVICE_PORT.TAG                          |
| FLAG                | FICON_DEVICE_PORT.FLAG                         |
| PARAMS              | FICON_DEVICE_PORT.PARAMS                       |
| NAME                | USER_DEFINED_DEVICE_DETAIL.NAME                |
| USER DEFINED TYPE   | USER_DEFINED_DEVICE_DETAIL.TYPE                |
| IP ADDRESS          | USER_DEFINED_DEVICE_DETAIL.IP_ADDRESS          |
| CONTACT             | USER_DEFINED_DEVICE_DETAIL.CONTACT             |
| LOCATION            | USER_DEFINED_DEVICE_DETAIL.LOCATION            |
| DESCRIPTION         | USER_DEFINED_DEVICE_DETAIL.DESCRPTION          |
| USER DEFINED VALUE1 | USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE1 |
| USER DEFINED VALUE2 | USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE2 |
| USER DEFINED VALUE3 | USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE3 |

**TABLE 80**    DEVICE\_INFO

| Name                      | Source                     |
|---------------------------|----------------------------|
| DEVICE NODE ID            | DEVICE_NODE.ID             |
| DEVICE NODE WWN           | DEVICE_NODE.WWN            |
| DEVICE NODE TYPE          | DEVICE_NODE.TYPE           |
| DEVICE NODE SYMBOLIC NAME | DEVICE_NODE.SYMBOLIC_NAME  |
| DEVICE_TYPE               | DEVICE_NODE.DEVICE_TYPE    |
| FDMI_HOST_NAME            | DEVICE_NODE.FDMI_HOST_NAME |
| VENDOR                    | DEVICE_NODE.VENDOR         |
| CAPABILITY_               | VICE_NODE.CAPABILITY_      |
| AG                        | DEVICE_NODE.AG             |
| DEVICE PORT ID            | DEVICE_PORT.ID             |
| DEVICE PORT DOMAIN ID     | DEVICE_PORT.DOMAIN_ID      |
| DEVICE PORT WWN           | DEVICE_PORT.WWN            |
| NUMBER                    | DEVICE_PORT.NUMBER         |
| PORT_ID                   | DEVICE_PORT.PORT_ID        |

**TABLE 80** DEVICE\_INFO (Continued)

| Name                      | Source                          |
|---------------------------|---------------------------------|
| DEVICE_PORT_TYPE          | DEVICE_PORT.TYPE                |
| DEVICE_PORT_SYMBOLIC_NAME | DEVICE_PORT.SYMBOLIC_NAME       |
| FC4_TYPE                  | DEVICE_PORT.FC4_TYPE,           |
| IP_PORT                   | DEVICE_PORT.IP_PORT             |
| HARDWARE_ADDRESS          | DEVICE_PORT.HARDWARE_ADDRESS    |
| DEVICE_PORT_TRUSTED       | DEVICE_PORT.TRUSTED             |
| DEVICE_PORT_MISSING       | DEVICE_PORT.MISSING             |
| COS                       | DEVICE_PORT.COS                 |
| NPV_PHYSICAL              | DEVICE_PORT.NPV_PHYSICAL        |
| SWITCH_PORT_ID            | SWITCH_PORT.ID                  |
| SWITCH_PORT_WWN           | SWITCH_PORT.WWN                 |
| SWITCH_PORT_NAME          | SWITCH_PORT.NAME                |
| SLOT_NUMBER               | SWITCH_PORT.SLOT_NUMBER         |
| PORT_NUMBER               | SWITCH_PORT.PORT_NUMBER         |
| PORT_INDEX                | SWITCH_PORT.PORT_INDEX          |
| SWITCH_PORT_TYPE          | SWITCH_PORT.TYPE                |
| SWITCH_PORT_FULL_TYPE     | SWITCH_PORT.FULL_TYPE           |
| SWITCH_PORT_STATUS        | SWITCH_PORT.STATUS              |
| SWITCH_PORT_HEALTH        | SWITCH_PORT.HEALTH              |
| SPEED                     | SWITCH_PORT.SPEED               |
| MAX_PORT_SPEED            | SWITCH_PORT.MAX_PORT_SPEED      |
| NPIV                      | SWITCH_PORT.NPIV                |
| NPIV_CAPABLE              | SWITCH_PORT.NPIV_CAPABLE        |
| CALCULATED_STATUS         | SWITCH_PORT.CALCULATED_STATUS   |
| AREA_ID                   | SWITCH_PORT.AREA_ID             |
| PHYSICAL_PORT             | SWITCH_PORT.PHYSICAL_PORT       |
| CATEGORY                  | SWITCH_PORT.CATEGORY            |
| PERSISTENT_DISABLE        | SWITCH_PORT.PERSISTENT_DISABLE  |
| BLOCKED                   | SWITCH_PORT.BLOCKED             |
| FCR_INTEROP_MODE          | SWITCH_PORT.FCR_INTEROP_MODE    |
| IP_ADDRESS                | SWITCH_INFO.IP_ADDRESS          |
| PHYSICAL_SWITCH_WWN       | SWITCH_INFO.PHYSICAL_SWITCH_WWN |
| FIRMWARE_VERSION          | SWITCH_INFO.FIRMWARE_VERSION    |
| REACHABLE                 | SWITCH_INFO.REACHABLE           |
| SYSLOG_REGISTERED         | SWITCH_INFO.SYSLOG_REGISTERED   |
| SNMP_REGISTERED           | SWITCH_INFO.SNMP_REGISTERED     |

**TABLE 80** DEVICE\_INFO (Continued)

| Name                     | Source                         |
|--------------------------|--------------------------------|
| VIRTUAL SWITCH ID        | SWITCH_INFO.ID                 |
| VIRTUAL SWITCH NAME      | SWITCH_INFO.NAME               |
| OPERATIONAL STATUS       | SWITCH_INFO.OPERATIONAL_STATUS |
| SWITCH_MODE              | SWITCH_INFO.SWITCH_MODE        |
| VIRTUAL SWITCH WWN       | SWITCH_INFO.WWN                |
| VIRTUAL SWITCH DOMAIN ID | SWITCH_INFO.DOMAIN_ID          |
| VIRTUAL_FABRIC_ID        | SWITCH_INFO.VIRTUAL_FABRIC_ID  |
| BASE_SWITCH              | SWITCH_INFO.BASE_SWITCH        |
| VIRTUAL SWITCH STATE     | SWITCH_INFO.STATE              |
| VIRTUAL SWITCH STATUS    | SWITCH_INFO.STATUS             |
| FABRIC ID                | SWITCH_INFO.FABRIC_ID          |
| CRYPTO_CAPABLE           | SWITCH_INFO.CRYPTO_CAPABLE     |

**TABLE 81** USER\_DEEFINED\_DEVICE\_DETAIL

| Field                | Definition                                  | Format  | Size |
|----------------------|---------------------------------------------|---------|------|
| WWN*                 | Device node or device port WWN.             | char    | 23   |
| NAME                 | User-assigned device name.                  | varchar | 256  |
| TYPE                 | User set device type (initiator or target). | varchar | 32   |
| IP_ADDRESS           | Device IP address.                          | varchar | 256  |
| CONTACT              | User-assigned contact.                      | varchar | 256  |
| LOCATION             | User-assigned device location.              | varchar | 256  |
| DESCRIPTION          | User-assigned description.                  | varchar | 256  |
| USER_DEFINED_VALUE1  | User-assigned arbitrary value.              | varchar | 256  |
| USEER_DEFINED_VALUE2 | User-assigned arbitrary value.              | varchar | 256  |
| USER_DEFINED_VALUE3  | User-assigned arbitrary value.              | varchar | 256  |

**TABLE 82** DEVICE\_NODE\_INFO

| Name           | Source                     |
|----------------|----------------------------|
| ID             | DEVICE_NODE.ID             |
| FABRIC ID      | DEVICE_NODE.FABRIC_ID      |
| WWN            | DEVICE_NODE.WWN            |
| TYPE           | DEVICE_NODE.TYPE           |
| DEVICE TYPE    | DEVICE_NODE.DEVICE_TYPE    |
| SYMBOLIC NAME  | DEVICE_NODE.SYMBOLIC_NAME  |
| FDMI HOST NAME | DEVICE_NODE.FDMI_HOST_NAME |
| VENDOR         | DEVICE_NODE.VENDOR         |

**TABLE 82** DEVICE\_NODE\_INFO (Continued)

| Name                | Source                                         |
|---------------------|------------------------------------------------|
| CAPABILITY          | DEVICE_NODE.CAPABILITY_                        |
| TRUSTED             | DEVICE_NODE.TRUSTED                            |
| CREATION TIME       | DEVICE_NODE.CREATION_TIME                      |
| MISSING             | DEVICE_NODE.MISSING                            |
| MISSING TIME        | DEVICE_NODE.MISSING_TIME,                      |
| PROXY DEVICE        | DEVICE_NODE.PROXY_DEVICE                       |
| AG                  | DEVICE_NODE.AG,                                |
| NAME                | USER_DEFINED_DEVICE_DETAIL.NAME                |
| USER DEFINED TYPE   | USER_DEFINED_DEVICE_DETAIL.TYPE                |
| IP ADDRESS          | USER_DEFINED_DEVICE_DETAIL.IP_ADDRESS          |
| CONTACT             | USER_DEFINED_DEVICE_DETAIL.CONTACT             |
| LOCATION            | USER_DEFINED_DEVICE_DETAIL.LOCATION            |
| DESCRIPTION         | USER_DEFINED_DEVICE_DETAIL.DESCRPTION          |
| USER DEFINED VALUE1 | USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE1 |
| USER DEFINED VALUE2 | USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE2 |
| USER DEFINED VALUE3 | USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE3 |

## EE- Monitor

**TABLE 83** EE\_MONITOR\_STATS

| Field         | Definition                                       | Format              | Size |
|---------------|--------------------------------------------------|---------------------|------|
| ID*           |                                                  | int                 |      |
| EE_MONITOR_ID | References to the ID in EE_MONITOR table.        | int                 |      |
| CREATION_TIME | The polling time.                                | timestamp           |      |
| ACTIVE_STATE  | State of collection<br>0 = failed<br>1 = success | smallint            |      |
| TX            | Transmit (TX) value in bytes.                    | double<br>precision |      |
| RX            | Receive (RX) value in bytes.                     | double<br>precision |      |
| CRCERRORS     | Number of CRC errors.                            | double              |      |

**TABLE 84** EE\_MONITOR\_STATS\_30MIN

| Field         | Definition | Format           | Size |
|---------------|------------|------------------|------|
| ID*           |            | int              |      |
| EE_MONITOR_ID |            | int              |      |
| CREATION_TIME |            | timestamp        |      |
| ACTIVE_STATE  |            | smallint         |      |
| TX            |            | double precision |      |
| RX            |            | double precision |      |
| CRCERRORS     |            | double           |      |

**TABLE 85** EE\_MONITOR\_STATS\_2HOUR

| Field         | Definition | Format           | Size |
|---------------|------------|------------------|------|
| ID*           |            | int              |      |
| EE_MONITOR_ID |            | int              |      |
| CREATION_TIME |            | timestamp        |      |
| ACTIVE_STATE  |            | smallint         |      |
| TX            |            | double precision |      |
| RX            |            | double precision |      |
| CRCERRORS     |            | double           |      |

**TABLE 86** EE\_MONITOR

| Field          | Definition                                                                                     | Format   | Size |
|----------------|------------------------------------------------------------------------------------------------|----------|------|
| ID*            |                                                                                                | int      |      |
| MONITOR_ID     | The Number (Index) given by the switch when user creates End-End monitor on the switch.        | int      |      |
| SWITCH_PORT_ID | References the ID in SWITCH_PORT table.                                                        | int      |      |
| SOURCE_PORT_ID | References the ID in DEVICE_PORT table and this is an initiator for EE monitor.                | int      |      |
| DEST_PORT_ID   | References the ID in DEVICE_PORT table and this is a target for EE monitor.                    | int      |      |
| NAME           | Name of the End_End Monitor.                                                                   | varchar  | 124  |
| ERROR CODE     | Error code returned from the switch, when enabling End-End monitor is attempted on the switch. | int      |      |
| STATUS         | Status of creating the End-End monitor on the switch. It can be either failed or succeeded.    | smallint |      |

**TABLE 87** EE\_MONITOR\_STATS\_1DAY

| Field         | Definition | Format | Size |
|---------------|------------|--------|------|
| ID*           |            | int    |      |
| EE_MONITOR_ID |            | int    |      |

**TABLE 87** EE\_MONITOR\_STATS\_1DAY (Continued)

| Field         | Definition | Format           | Size |
|---------------|------------|------------------|------|
| CREATION_TIME |            | timestamp        |      |
| ACTIVE_STATE  |            | smallint         |      |
| TX            |            | double precision |      |
| RX            |            | double precision |      |
| CRCERRORS     |            | double           |      |

## Event/FM

**TABLE 88** RECIPIENT\_TYPE

| Field | Definition                              | Format  | Size |
|-------|-----------------------------------------|---------|------|
| ID*   |                                         | int     |      |
| TYPE  | Type of the recipient (Syslog or SNMP). | varchar | 20   |

**TABLE 89** SOURCE\_OBJECT\_TYPE

| Field       | Definition                                                                     | Format  | Size |
|-------------|--------------------------------------------------------------------------------|---------|------|
| ID*         |                                                                                | int     |      |
| TYPE_NAME   | Type of the object to which the event applies, such as Fabric, Switch or Port. | char    | 64   |
| DESCRIPTION | Description of the object                                                      | varchar | 255  |

**TABLE 90** EVENT\_TYPE

| Field       | Definition                     | Format  | Size |
|-------------|--------------------------------|---------|------|
| ID*         |                                | int     |      |
| TYPE_CODE   | Event Type Code.               | char    | 64   |
| DESCRIPTION | Description of the Event Rule. | varchar | 255  |

**TABLE 91** MESSAGE\_RECIPIENT

| Field             | Definition                       | Format  | Size |
|-------------------|----------------------------------|---------|------|
| ID*               |                                  | int     |      |
| DESCRIPTION       | Description about recipient.     | varchar | 64   |
| IP_ADDRESS        | IP Address of the recipient.     | varchar | 128  |
| PORT              | Port number of the recipient.    | int     |      |
| RECIPIENT_TYPE_ID | Recipient Type (Syslog or SNMP). | int     |      |

**TABLE 92** EVENT\_SUB\_TYPE

| Field         | Definition                    | Format  | Size |
|---------------|-------------------------------|---------|------|
| ID*           |                               | int     |      |
| EVENT_TYPE_ID | Unique Event Sub type ID      | int     |      |
| DESCRIPTION   | Description of Event Sub Type | varchar | 255  |

**TABLE 93** SNMP\_CREDENTIALS

| Field                  | Definition                                                                                                                                                                                                                                                                                                            | Format   | Size |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                    |                                                                                                                                                                                                                                                                                                                       | int      |      |
| VIRTUAL_SWITCH_ID      | Virtual switch ID for which this instance of the SNMP credentials apply.                                                                                                                                                                                                                                              | int      |      |
| RECIPIENT_ID           | Refers to recipient in the MESSAGE_RECIPIENT table.                                                                                                                                                                                                                                                                   | int      | 255  |
| PORT_NUMBER            | Port number of the SNMP agent on the switch for get and set requests.                                                                                                                                                                                                                                                 | smallint |      |
| RETRY_COUNT            | Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.                                                                                                                                                                                                                          | smallint |      |
| TIMEOUT                | Timeout value in seconds for a get/set request to the SNMP agent. Default value is 5.                                                                                                                                                                                                                                 | smallint |      |
| VERSION                | SNMP agent version running on the switch, as in SNMPv1 or SNMPv3.                                                                                                                                                                                                                                                     | varchar  | 6    |
| READ_COMMUNITY_STRING  | The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to a device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.                                                                     | varchar  | 64   |
| WRITE_COMMUNITY_STRING | The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1.                                                                     | varchar  | 64   |
| USER_NAME              | A human-readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                                                                                        | varchar  | 64   |
| CONTEXT_NAME           | Text ID associated with the user, used by SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                                                                  | varchar  | 128  |
| AUTH_PROTOCOL          | An indication of whether messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. Supported values are:<br>usmNoAuthProtocol<br>usmHMACMD5AuthProtocol<br>usmHMACSHAAuthProtocol<br>This is applicable if the agent is configured to operate in SNMPv3. | varchar  | 16   |

**TABLE 93** SNMP\_CREDENTIALS (Continued)

| Field         | Definition                                                                                                                                                                                                                                                                   | Format  | Size |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|
| AUTH_PASSWORD | The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                | varchar | 64   |
| PRIV_PROTOCOL | An indication of whether messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. Supported values are:<br>usmNoPrivProtocol<br>usmDESPrivProtocol<br>This is applicable if the agent is configured to operate in SNMPv3. | varchar | 16   |
| PRIV_PASSWORD | The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                            | varchar | 64   |

**TABLE 94** SYSLOG\_EVENT

| Field                       | Definition                                    | Format    | Size |
|-----------------------------|-----------------------------------------------|-----------|------|
| ID*                         |                                               | int       |      |
| SWITCH_ID                   | Switch ID.                                    | int       |      |
| SOURCE_NAME                 | Source Name from which the event originated.  | varchar   | 32   |
| SOURCE_ADDR                 | IP Address from which the event originated.   | varchar   | 32   |
| EVENT_SOURCE                | Source from which the event is generated.     | varchar   | 32   |
| STATUS                      | Status of the event.                          | varchar   | 32   |
| PRIORITY                    | Priority of the event. Default priority is 7. | int       |      |
| EVENT_NUMBER                | Sequence number of the event.                 | int       |      |
| EVENT_COUNT                 | Number of occurrences of the event.           | int       |      |
| AUDIT                       | Audit file of the syslog message.             | varchar   | 10   |
| FIRST_OCCURENCE_SWITCH_TIME | First occurrence switch time.                 | timestamp |      |
| LAST_OCCURENCE_SWITCH_TIME  | Last occurrence switch time.                  | timestamp |      |
| FIRST_OCCURENCE_HOST_TIME   | Last occurrence switch time.                  | timestamp |      |
| LAST_OCCURENCE_HOST_TIME    | Last occurrence host time.                    | timestamp |      |
| MODULE                      | Module of the event.                          | varchar   | 10   |
| MESSAGE_ID                  | Message ID of the event.                      | varchar   | 20   |
| DESCRIPTION                 | Description of the event.                     | varchar   | 512  |
| PROBABLE_CAUSE              | Probable root cause of the event.             | varchar   | 512  |
| RECOMMENDED_ACTION          | Recommended action for the event.             | varchar   | 512  |
| CONTRIBUTORS                | Contributors of the syslog event.             | varchar   | 512  |

**TABLE 95** EVENT

| Field                       | Definition                                                                                                        | Format    | Size |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------|-----------|------|
| ID*                         |                                                                                                                   | int       |      |
| SWITCH_ID                   | ID of the switch.                                                                                                 | int       |      |
| PARENT_ID                   | ID of the Parent.                                                                                                 | int       | 255  |
| SOURCE_NAME                 | Name of the source from which the event originated.                                                               | varchar   | 32   |
| SOURCE_ADDR                 | IP Address of the source from which the event originated.                                                         | varchar   | 50   |
| EVENT_SOURCE                | Source from which the event is generated.                                                                         | varchar   | 32   |
| SINK_SOURCE                 | Sink Source of the event (Syslog/SNMP Trap/errlog/Application).                                                   | varchar   | 32   |
| STATUS                      | Status of the event (Down/Marginal/Healthy).                                                                      | varchar   | 32   |
| PRIORITY                    | Event priority, by default the value will be 7 (Unknown).                                                         | int       |      |
| EVENT_NUMBER                | Sequence number of the event. A Sequence number is received from certain events, but for others it defaults to 0. | int       |      |
| EVENT_COUNT                 | Number of occurrences of the event.                                                                               | int       |      |
| AUDIT                       | Flag to indicate if the event is audited.                                                                         | varchar   | 10   |
| FIRST_OCCURENCE_SWITCH_TIME | First occurrence switch time.                                                                                     | timestamp |      |
| LAST_OCCURENCE_SWITCH_TIME  | Last occurrence switch time.                                                                                      | timestamp |      |
| FIRST_OCCURENCE_HOST_TIME   | First occurrence host time; this is set to GMT time.                                                              | timestamp |      |
| LAST_OCCURENCE_HOST_TIME    | Last occurrence host time; this is set to GMT time.                                                               | timestamp |      |
| MODULE                      | Module from which the event is generated.                                                                         | varchar   | 20   |
| MESSAGE_ID                  | Unique message ID of the event.                                                                                   | varchar   | 20   |
| DESCRIPTION                 | Description of the event.                                                                                         | varchar   | 512  |
| RESOLVED                    | Resolution status of the event.                                                                                   | smallint  |      |
| ACKNOWLEDGED                | Acknowledgement status of the event.                                                                              | smallint  |      |
| ACKED_BY                    | User who acknowledged the event                                                                                   | varchar   | 80   |
| ACKED_TIME                  | Time at which the event is acknowledged                                                                           | timestamp |      |
| PORABLE_CAUSE               | Probable root cause of the event                                                                                  | varchar   | 512  |
| RECOMMENDED_ACTION          | Recommended action for the event                                                                                  | varchar   | 512  |
| CONTRIBUTORS                | Contributors of the event                                                                                         | varchar   | 512  |
| SOURCE_OBJECT_ID            | Source Object ID                                                                                                  | int       |      |
| SOURCE_OBJECT_TYPE_ID       | Source Object type                                                                                                | int       |      |
| EVENT_TYPE_ID               | Event Type ID of the event                                                                                        | int       |      |
| EVENT_SUB_TYPE_ID           | Sub Type ID of the event                                                                                          | int       |      |

**TABLE 95** EVENT (Continued)

| Field              | Definition                                                                            | Format    | Size |
|--------------------|---------------------------------------------------------------------------------------|-----------|------|
| EVENT_CATEGORY     | Category of the event                                                                 | varchar   | 64   |
| DISCOVERY_TYPE     | Discovery type of the product                                                         | varchar   | 64   |
| MANAGEMENT_LINK    | Management link status                                                                | varchar   | 255  |
| OPERATIONAL_STATUS | Operational Status of the switch from which the event is triggered                    | varchar   | 255  |
| NODE_WWN           | WWN of the node from which the event is triggered                                     | varchar   | 23   |
| PORT_WWN           | WWN of the port from which the event is triggered                                     | varchar   | 23   |
| NODE_NAME          | Node Name from which the event is triggered                                           | varchar   | 255  |
| PORT_NAME          | Port Name from which the event is triggered                                           | varchar   | 255  |
| RESOLVED_TIME      | Time at which the event is resolved                                                   | timestamp |      |
| FRU_CODE           | FRU Code used for call home                                                           | int       |      |
| REASON_CODE        | Event Reason code to identify the event uniquely                                      | int       |      |
| FRU_POSITION       | Failed FRU position in case of FRU failure, 0 otherwise                               | int       |      |
| CALL_HOME          | Call Home status of the Event.<br>1 = call home event.<br>0 = not a call home event.  | smallint  |      |
| OID                | Object Identifier of the SNMP Trap Event. For other events, this column will be blank | varchar   | 50   |

**TABLE 96** RAS\_LOG

| Field      | Definition                         | Format  | Size |
|------------|------------------------------------|---------|------|
| MSG_ID*    | Message ID of the event.           | varchar | 15   |
| MODULE_ID  | Module ID of the event.            | varchar | 10   |
| SEVERITY   | Severity of the event.             | varchar | 10   |
| CAUSE      | Probable root cause for the event. | varchar | 4096 |
| ACTION     | Recommended action for the event.  | varchar | 4096 |
| OLD_MSG_ID | Old message ID.                    | varchar | 45   |

**TABLE 97** EVENT\_NOTIFICATION

| Field         | Definition                                                              | Format   | Size |
|---------------|-------------------------------------------------------------------------|----------|------|
| ID*           |                                                                         | int      |      |
| STATUS        | Status of Event Notification. value will be 0 if disabled, 1 otherwise. | smallint |      |
| SERVER_NAME   | E-mail (SMTP) server name.                                              | varchar  | 256  |
| REPLY_ADDRESS | Reply E-mail address.                                                   | varchar  | 50   |
| SEND_ADDRESS  | E-mail address for which a Test E-mail notification is to be sent.      | varchar  | 512  |
| SMTP_PORT     | SMTP Port number.                                                       | int      |      |

**TABLE 97** EVENT\_NOTIFICATION (Continued)

| Field                 | Definition                                                                                                | Format   | Size |
|-----------------------|-----------------------------------------------------------------------------------------------------------|----------|------|
| USER_NAME             | User name for authentication.                                                                             | varchar  | 256  |
| PASSWORD              | Password for authentication.                                                                              | varchar  | 256  |
| NOTIFICATION_INTERVAL | Time interval between successive event notifications.                                                     | int      |      |
| NOTIFICATION_UNIT     | Time interval Unit:<br>0 = Seconds<br>1 = Minutes<br>2 = Hours                                            | smallint |      |
| TEST_OPTION           | Time interval Unit:<br>0 = Send test to configured e-mail address.<br>1 = Send test to all enabled users. | smallint |      |

**TABLE 98** EVENT\_RULE

| Field                | Definition                                                                                              | Format   | Size |
|----------------------|---------------------------------------------------------------------------------------------------------|----------|------|
| ID*                  |                                                                                                         | int      |      |
| NAME                 | Name of the Event Rule.                                                                                 | varchar  | 255  |
| TYPE                 | Event Rule Type:<br>0 = Port Offline<br>1 = PM Threshold crossed<br>2 = Security Violation<br>4 = Event | int      |      |
| DESCRIPTION          | Description about the Event Rule.                                                                       | varchar  | 512  |
| OPERATOR1            | AND operator used to append the rule.                                                                   | varchar  | 12   |
| EVENT_TYPE_ID        | The Selected Event type ID from the Event type combo box.                                               | int      |      |
| OPERATOR2            | AND operator used to append the rule.                                                                   | varchar  | 12   |
| MESSAGE_ID           | Message ID provided by the user.                                                                        | varchar  | 20   |
| OPERATOR3            | AND operator used to append the rule.                                                                   | varchar  | 12   |
| IP_ADDRESS           | Source IP Address.                                                                                      | varchar  | 32   |
| OPERATOR4            | AND operator used to append the rule.                                                                   | varchar  | 12   |
| WWN                  | Source WWN.                                                                                             | varchar  | 255  |
| OPERATOR5            | AND operator used to append the rule.                                                                   | varchar  | 12   |
| COUNT                | Count of the specified event.                                                                           | int      |      |
| OPERATOR6            | AND operator used to append the rule.                                                                   | varchar  | 12   |
| DURATION             | Duration of the specified event.                                                                        | bigint   |      |
| STATE                | State of the rule:<br>0 = Disabled<br>1 = Enabled                                                       | smallint |      |
| SEVERITY_LEVEL       | Event severity level.                                                                                   | int      |      |
| SOURCE_NAME          | Name of the source.                                                                                     | varchar  | 255  |
| DESCRIPTION_CONTAINS | Description pattern about the rule.                                                                     | varchar  | 255  |

**TABLE 98** EVENT\_RULE (Continued)

| Field              | Definition                                                                     | Format    | Size |
|--------------------|--------------------------------------------------------------------------------|-----------|------|
| LAST_MODIFIED_TIME | Rules last edited time.                                                        | timestamp |      |
| SELECTED_TIME_UNIT | Timestamp unit of the selected rule:<br>0 = second<br>1 = Minutes<br>2 = Hours | smallint  |      |

**TABLE 99** EVENT\_RULE\_ACTION

| Field   | Definition                                                                                                                                  | Format   | Size |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*     |                                                                                                                                             | int      |      |
| RULE_ID | The rule ID present in the Event_Rule Table.                                                                                                | int      |      |
| NAME    | Name of the Event Rule Action:<br>Launch Script = for launch script<br>Send E-mail = for send e-mail<br>Raise Event = for broadcast message | varchar  | 255  |
| TYPE    | Name of the action:<br>script = for Launch Script<br>e-mail = for E-mail<br>message = for Broadcast message                                 | varchar  | 30   |
| FIELD1  | Data for the selected action.                                                                                                               | varchar  | 512  |
| FIELD2  | Data for the selected action.                                                                                                               | varchar  | 512  |
| FIELD3  | Data for the selected action.                                                                                                               | varchar  | 512  |
| FIELD4  | Data for the selected action.                                                                                                               | varchar  | 512  |
| STATE   | State of the Action:<br>0 = Action Disabled<br>1 = Action Enabled                                                                           | smallint |      |

## Fabric

**TABLE 100** SAN

| Field            | Definition                                          | Format    | Size |
|------------------|-----------------------------------------------------|-----------|------|
| ID*              |                                                     | int       |      |
| NAME             | Name of this SAN.                                   | varchar   | 256  |
| CONTACT          | Contact person for this SAN.                        | varchar   | 256  |
| LOCATION         | Location of this SAN.                               | varchar   | 256  |
| DESCRIPTION      | Description.                                        | varchar   | 256  |
| STATS_COLLECTION | 1 = statistics collection is enabled; otherwise, 0. | smallint  |      |
| CREATION_TIME    | time at which this record was created.              | timestamp |      |
| LAST_UPDATE_TIME | time when this was last updated.                    | timestamp |      |

**TABLE 101** FABRIC

| Field                | Definition                                                                          | Format    | Size |
|----------------------|-------------------------------------------------------------------------------------|-----------|------|
| ID*                  |                                                                                     | int       |      |
| SAN_ID               | Foreign key to SAN table; usually 1 since there is only one SAN.                    | int       |      |
| SEED_SWITCH_WWN      | WWN of the virtual switch used as seed switch to discover the fabric.               | char      | 23   |
| NAME                 | User-assigned fabric name.                                                          | varchar   | 256  |
| CONTACT              | User-assigned "contact" for the fabric.                                             | varchar   | 256  |
| LOCATION             | User-assigned "location" for the fabric.                                            | varchar   | 256  |
| DESCRIPTION          | User-assigned fabric description.                                                   | varchar   | 256  |
| TYPE                 | Type of fabric:<br>0 = legacy fabric<br>1 = base fabric<br>2 = logical fabric       | smallint  |      |
| SECURE               | 1 = it is a secured fabric.                                                         | smallint  |      |
| AD_ENVIRONMENT       | 1 = there are user-defined ADs in this fabric.                                      | smallint  |      |
| MANAGED              | 1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric. | smallint  |      |
| MANAGEMENT_STATE     | Bit map to indicate various management indications for the fabric.                  | smallint  |      |
| TRACK_CHANGES        | 1 = changes (member switches, ISL and devices) in the fabric are tracked.           | smallint  |      |
| STATS_COLLECTION     | 1 = statistics collection is enabled on the fabric.                                 | smallint  |      |
| CREATION_TIME        | When the fabric record is inserted, i.e., created.                                  | timestamp |      |
| LAST_FABRIC_CHANGED  | Time when fabric last changed.                                                      | timestamp |      |
| LAST_SCAN_TIME       |                                                                                     | timestamp |      |
| LAST_UPDATE_TIME     | Time when fabric was last updated.                                                  | timestamp |      |
| ACTIVE_ZONESET_NAME  | Name of the zone configuration which is effective / active in that fabric.          | varchar   | 256  |
| USER_DEFINED_VALUE_1 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_2 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_3 | User-defined custom value.                                                          | varchar   | 256  |

**TABLE 102** FABRIC\_INFO

| Name                | Source                     |
|---------------------|----------------------------|
| ID                  | FABRIC.ID                  |
| SAN_ID              | FABRIC.SAN_ID              |
| SEED_SWITCH_WWN     | FABRIC.SEED_SWITCH_WWN     |
| NAME                | FABRIC.NAME                |
| ACTIVE_ZONESET_NAME | FABRIC.ACTIVE_ZONESET_NAME |

**TABLE 102** FABRIC\_INFO (Continued)

| Name                   | Source                              |
|------------------------|-------------------------------------|
| MANAGEMENT_STATE       | FABRIC.MANAGEMENT_STATE             |
| LAST_FABRIC_CHANGED    | FABRIC.LAST_FABRIC_CHANGED          |
| SECURE                 | FABRIC.SECURE                       |
| AD_ENVIRONMENT         | FABRIC.AD_ENVIRONMENT               |
| MANAGED                | FABRIC.MANAGED                      |
| CONTACT                | FABRIC.CONTACT                      |
| LOCATION               | FABRIC.LOCATION                     |
| DESCRIPTION            | FABRIC.DESCRPTION                   |
| CREATION_TIME          | FABRIC.CREATION_TIME                |
| LAST_SCAN_TIME         | FABRIC.LAST_SCAN_TIME               |
| LAST_UPDATE_TIME       | FABRIC.LAST_UPDATE_TIME             |
| TRACK_CHANGES          | FABRIC.TRACK_CHANGES                |
| TYPE                   | FABRIC.TYPE                         |
| USER_DEFINED_VALUE_1   | FABRIC.USER_DEFINED_VALUE_1         |
| USER_DEFINED_VALUE_2   | FABRIC.USER_DEFINED_VALUE_2         |
| USER_DEFINED_VALUE_3   | FABRIC.USER_DEFINED_VALUE_3         |
| ID                     | VIRTUAL_SWITCH.ID                   |
| SEED SWITCH IP ADDRESS | CORE_SWITCH.IP_ADDRESS              |
| SWITCH COUNT           | FABRIC_MEMBER.FABRIC_ID = FABRIC.ID |

**TABLE 103** FABRIC\_MEMBER

| Field              | Definition                                                                                                                                        | Format    | Size |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| FABRIC_ID*         | Fabric ID, foreign key to FABRIC table.                                                                                                           | INT       |      |
| VIRTUAL_SWITCH_ID* | ID of the virtual switch which is a member of this fabric, foreign key to VIRTUAL_SWITCH table.                                                   | INT       |      |
| TRUSTED            | 1 = the switch is a trusted member of the fabric. Either found in the initial discovery or user subsequently entrusted the switch by user action. | SMALLINT  |      |
| CREATION_TIME      | When the switch became a member.                                                                                                                  | TIMESTAMP |      |
| MISSING            | 1 = it is missing from the fabric.                                                                                                                | SMALLINT  |      |
| MISSING_TIME       | When it is missed from the fabric; null if the member is entrusted.                                                                               | TIMESTAMP |      |

## FC Port Stats

**TABLE 104** FC\_PORT\_STATS

| Field                | Definition                                        | Format    | Size |
|----------------------|---------------------------------------------------|-----------|------|
| ID*                  |                                                   | int       |      |
| SWITCH_ID            | References the ID in CORE_SWITCH table.           | int       |      |
| PORT_ID              | References the ID in SWITCH_PORT table.           | int       |      |
| TX                   | Transmission (TX) value in bytes.                 | double    |      |
| RX                   | Receive (RX) value in bytes.                      | double    |      |
| TX_UTILIZATION       | Transmit utilization value in percentage.         | double    |      |
| RX_UTILIZATION       | Receive utilization value in percentage.          | double'   |      |
| CREATION_TIME        | The polling time.                                 | timestamp |      |
| ACTIVE_STATE         | State of collection:<br>0 = failed<br>1 = success | smallint  |      |
| LINKFAILURES         | Number of link failures.                          | double    |      |
| TXLINKRESETS         | Number of transmit link failures.                 | double    |      |
| RXLINKRESETS         | Number of receive link failures.                  | double    |      |
| SYNCLOSSES           | Number of sync losses.                            | double    |      |
| SIGNALLOSSES         | Number of signal losses.                          | double    |      |
| SEQUENCEERRORS       | Number of sequence errors.                        | double    |      |
| INVALIDTRANSMISSIONS | Number of invalid transmission errors.            | double    |      |
| CRCERRORS            | Number of CRC errors.                             | double    |      |

**TABLE 105** FC\_PORT\_STATS\_30MIN

| Field          | Definition | Format    | Size |
|----------------|------------|-----------|------|
| ID*            |            | int       |      |
| SWITCH_ID      |            | int       |      |
| PORT_ID        |            | int       |      |
| TX             |            | double    |      |
| RX             |            | double    |      |
| TX_UTILIZATION |            | double    |      |
| RX_UTILIZATION |            | double'   |      |
| CREATION_TIME  |            | timestamp |      |
| ACTIVE_STATE   |            | smallint  |      |
| LINKFAILURES   |            | double    |      |
| TXLINKRESETS   |            | double    |      |
| RXLINKRESETS   |            | double    |      |
| SYNCLOSSES     |            | double    |      |

**TABLE 105** FC\_PORT\_STATS\_30MIN (Continued)

| Field                | Definition | Format   | Size |
|----------------------|------------|----------|------|
| SIGNALLOSSES         |            | double   |      |
| SEQUENCEERRORS       |            | double   |      |
| INVALIDTRANSMISSIONS |            | double   |      |
| CRCERRORS            |            | double   |      |
| DATA_GAPS_IN5MIN     |            | smallint |      |

**TABLE 106** FC\_PORT\_STATS\_2HOUR

| Field                | Definition | Format    | Size |
|----------------------|------------|-----------|------|
| ID*                  |            | int       |      |
| SWITCH_ID            |            | int       |      |
| PORT_ID              |            | int       |      |
| TX                   |            | double    |      |
| RX                   |            | double    |      |
| TX_UTILIZATION       |            | double    |      |
| RX_UTILIZATION       |            | double    |      |
| CREATION_TIME        |            | timestamp |      |
| ACTIVE_STATE         |            | smallint  |      |
| LINKFAILURES         |            | double    |      |
| TXLINKRESETS         |            | double    |      |
| RXLINKRESETS         |            | double    |      |
| SYNCLOSSES           |            | double    |      |
| SIGNALLOSSES         |            | double    |      |
| SEQUENCEERRORS       |            | double    |      |
| INVALIDTRANSMISSIONS |            | double    |      |
| CRCERRORS            |            | double    |      |
| DATA_GAPS_IN5MIN     |            | smallint  |      |
| DATA_GAPS_IN30MIN    |            | smallint  |      |

**TABLE 107** FC\_PORT\_STATS\_1DAY

| Field          | Definition | Format | Size |
|----------------|------------|--------|------|
| ID*            |            | int    |      |
| SWITCH_ID      |            | int    |      |
| PORT_ID        |            | int    |      |
| TX             |            | double |      |
| RX             |            | double |      |
| TX_UTILIZATION |            | double |      |

**TABLE 107** FC\_PORT\_STATS\_1DAY (Continued)

| Field                | Definition | Format    | Size |
|----------------------|------------|-----------|------|
| RX_UTILIZATION       |            | double    |      |
| CREATION_TIME        |            | timestamp |      |
| ACTIVE_STATE         |            | smallint  |      |
| LINKFAILURES         |            | double    |      |
| TXLINKRESETS         |            | double    |      |
| RXLINKRESETS         |            | double    |      |
| SYNCLOSSES           |            | double    |      |
| SIGNALLOSSES         |            | double    |      |
| SEQUENCEERRORS       |            | double    |      |
| INVALIDTRANSMISSIONS |            | double    |      |
| CRCERRORS            |            | double    |      |
| DATA_GAPS_IN5MIN     |            | smallint  |      |
| DATA_GAPS_IN30MIN    |            | smallint  |      |
| DATA_GAPS_IN2HOUR    |            | smallint  |      |

## FCIP

**TABLE 108** FCIP\_TUNNEL

| Field                      | Definition                                   | Format   | Size |
|----------------------------|----------------------------------------------|----------|------|
| ID*                        |                                              | int      |      |
| ETHERNET_PORT_ID           | GigE Port ID on which the tunnel is created. | int      |      |
| TUNNEL_ID                  | Tunnel ID for that GigE Port.                | smallint |      |
| VLAN_TAG                   | VLAN Tag on the tunnel (if present).         | int      |      |
| SOURCE_IP                  | Source IP on which the tunnel is created.    | char     | 64   |
| DEST_IP                    | Destination IP on the other end of tunnel.   | char     | 64   |
| LOCAL_WWN                  | Local port WWN for the tunnel.               | char     | 23   |
| REMOTE_WWN_RESTRICT        | Remote Port WWN for the tunnel.              | char     | 23   |
| COMMUNICATION_RATE         | Bandwidth specified for the tunnel.          | double   |      |
| MIN_RETRANSMIT_TIME        | FCIP Tunnel Parameter.                       | int      |      |
| SELECTIVE_ACK_ENABLED      | FCIP Tunnel Parameter.                       | smallint |      |
| KEEP_ALIVE_TIMEOUT         | FCIP Tunnel Parameter.                       | int      |      |
| MAX_RETRNASMISSION         | FCIP Tunnel Parameter.                       | int      |      |
| PATH_MTU_DISCOVERY_ENABLED | FCIP Tunnel Parameter.                       | smallint |      |
| WAN_TOV_ENABLED            | FCIP Tunnel Parameter.                       | smallint |      |
| TUNNEL_STATUS              | Tunnel Status (Active/Inactive).             | int      |      |

**TABLE 109** FCIP\_TUNNEL\_INFO

| Name                       | Source                                 |
|----------------------------|----------------------------------------|
| ID                         | FCIP_TUNNEL.ID                         |
| ETHERNET_PORT_ID           | FCIP_TUNNEL.ETHERNET_PORT_ID           |
| TUNNEL_ID                  | FCIP_TUNNEL.TUNNEL_ID                  |
| VLAN_TAG                   | FCIP_TUNNEL.VLAN_TAG                   |
| SOURCE_IP                  | FCIP_TUNNEL.SOURCE_IP                  |
| DEST_IP                    | FCIP_TUNNEL.DEST_IP                    |
| LOCAL_WWN                  | FCIP_TUNNEL.LOCAL_WWN                  |
| REMOTE_WWN_RESTRICT        | FCIP_TUNNEL.REMOTE_WWN_RESTRICT        |
| COMMUNICATION_RATE         | FCIP_TUNNEL.COMMUNICATION_RATE         |
| MIN_RETRANSMIT_TIME        | FCIP_TUNNEL.MIN_RETRANSMIT_TIME        |
| SELECTIVE_ACK_ENABLED      | FCIP_TUNNEL.SELECTIVE_ACK_ENABLED      |
| KEEP_ALIVE_TIMEOUT         | FCIP_TUNNEL.KEEP_ALIVE_TIMEOUT         |
| MAX_RETRNASMISSION         | FCIP_TUNNEL.MAX_RETRANSMISSION         |
| PATH_MTU_DISCOVERY_ENABLED | FCIP_TUNNEL.PATH_MTU_DISCOVERY_ENABLED |

**TABLE 109** FCIP\_TUNNEL\_INFO (Continued)

| Name                                     | Source                                                                                                                |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| WAN_TOV_ENABLED                          | FCIP_TUNNEL.WAN_TOV_ENABLED                                                                                           |
| TUNNEL_STATUS                            | FCIP_TUNNEL.TUNNEL_STATUS                                                                                             |
| COMPRESSION_ENABLED                      | FCIP_TUNNEL_DETAILS.COMPRESSION_ENABLED                                                                               |
| TURBO_WRITE_ENABLED                      | FCIP_TUNNEL_DETAILS.TURBO_WRITE_ENABLED                                                                               |
| TAPE_ACCELERATION_ENABLED                | FCIP_TUNNEL_DETAILS.TAPE_ACCELERATION_ENABLED                                                                         |
| IKE_POLICY_NUM                           | FCIP_TUNNEL_DETAILS.IKE_POLICY_NUM                                                                                    |
| IPSEC_POLICY_NUM                         | FCIP_TUNNEL_DETAILS.IPSEC_POLICY_NUM                                                                                  |
| PRESHARED_KEY                            | FCIP_TUNNEL_DETAILS.PRESHARED_KEY                                                                                     |
| FICON_TAPE_READ_BLOCK_ID_ENABLED         | FCIP_TUNNEL_DETAILS.FICON_TAPE_READ_BLOCK_ID_ENABLED                                                                  |
| FICON_TIN_TIR_EMULATION_ENABLED          | FCIP_TUNNEL_DETAILS.FICON_TIN_TIR_EMULATION_ENABLED                                                                   |
| FICON_DEVICE_LEVEL_ACK_EMULATION_ENABLED | FCIP_TUNNEL_DETAILS.FICON_DEVICE_LEVEL_ACK_EMULATION_ENABLED                                                          |
| FICON_TAPE_WRITE_MAX_PIPE                | FCIP_TUNNEL_DETAILS.FICON_TAPE_WRITE_MAX_PIPE                                                                         |
| FICON_TAPE_READ_MAX_PIPE                 | FCIP_TUNNEL_DETAILS.FICON_TAPE_READ_MAX_PIPE                                                                          |
| FICON_TAPE_WRITE_MAX_OPS                 | FCIP_TUNNEL_DETAILS.FICON_TAPE_WRITE_MAX_OPS                                                                          |
| FICON_TAPE_READ_MAX_OPS                  | FCIP_TUNNEL_DETAILS.FICON_TAPE_READ_MAX_OPS                                                                           |
| FICON_TAPE_WRITE_TIMER                   | FCIP_TUNNEL_DETAILS.FICON_TAPE_WRITE_TIMER                                                                            |
| FICON_TAPE_MAX_WRITE_CHAIN               | FCIP_TUNNEL_DETAILS.FICON_TAPE_MAX_WRITE_CHAIN                                                                        |
| FICON_OXID_BASE                          | FCIP_TUNNEL_DETAILS.FICON_OXID_BASE                                                                                   |
| FICON_XRC_EMULATION_ENABLED              | FCIP_TUNNEL_DETAILS.FICON_XRC_EMULATION_ENABLED                                                                       |
| FICON_TAPE_WRITE_EMULATION_ENABLED       | FCIP_TUNNEL_DETAILS.FICON_TAPE_WRITE_EMULATION_ENABLED                                                                |
| FICON_TAPE_READ_EMULATION_ENABLED        | FCIP_TUNNEL_DETAILS.FICON_TAPE_READ_EMULATION_ENABLED                                                                 |
| FICON_DEBUG_FLAGS                        | FCIP_TUNNEL_DETAILS.FICON_DEBUG_FLAGS                                                                                 |
| SLOT_NUMBER                              | GIGE_PORT.SLOT_NUMBER                                                                                                 |
| SWITCH PORT ID                           | GIGE_PORT.PORT_NUMBER                                                                                                 |
| ID                                       | SWITCH_PORT.ID                                                                                                        |
| VIRTUAL_SWITCH_ID                        | SWITCH_PORT.VIRTUAL_SWITCH_ID                                                                                         |
| USER_PORT_NUMBER                         | SWITCH_PORT.USER_PORT_NUMBER                                                                                          |
| VIRTUAL PORT WWN                         | FCIP_PORT_TUNNEL_MAP.TUNNEL_ID = FCIP_TUNNEL.ID and<br>FCIP_PORT_TUNNEL_MAP.SWITCHPORT_ID = PORT.ID) VIRTUAL_PORT_WWN |

**TABLE 109** FCIP\_TUNNEL\_INFO (Continued)

| Name            | Source                                                                                                               |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| REMOTE PORT WWN | FCIP_PORT_TUNNEL_MAP.TUNNEL_ID = FCIP_TUNNEL.ID and<br>FCIP_PORT_TUNNEL_MAP.SWITCHPORT_ID = PORT.ID) REMOTE_PORT_WWN |
| REMOTE NODE WWN | FCIP_PORT_TUNNEL_MAP.TUNNEL_ID = FCIP_TUNNEL.ID and<br>FCIP_PORT_TUNNEL_MAP.SWITCHPORT_ID = PORT.ID) REMOTE_NODE_WWN |

**TABLE 110** FCIP\_PORT\_TUNNEL\_MAP

| Field          | Definition      | Format | Size |
|----------------|-----------------|--------|------|
| SWITCHPORT_ID* | Switch Port ID. | int    |      |
| TUNNEL_ID*     | FCIP Tunnel ID. | int    |      |

**TABLE 111** FCIP\_TUNNEL\_DETAILS

| Field                                    | Definition                                                    | Format   | Size |
|------------------------------------------|---------------------------------------------------------------|----------|------|
| TUNNEL_ID*                               | Tunnel ID for that GigE Port.                                 | int      |      |
| COMPRESSION_ENABLED                      | Whether Compression is enabled on that tunnel.                | smallint |      |
| TURBO_WRITE_ENABLED                      | Whether TurboWrite is enabled on that tunnel.                 | smallint |      |
| TAPE_ACCELERATION_ENABLED                | Whether TapeAcceleration is enabled on that tunnel.           | smallint |      |
| IKE_POLICY_NUM                           | The IKE Policy on the tunnel.                                 | int      |      |
| IPSEC_POLICY_NUM                         | The IPSEC Policy on the tunnel.                               | int      |      |
| PRESHARED_KEY                            | The Preshared Key on the tunnel.                              | char     | 32   |
| FICON_TAPE_READ_BLOCK_ID_ENABLED         | Whether Ficon_Tape_Read_Block is enabled on that tunnel.      | smallint |      |
| FICON_TIN_TIR_EMULATION_ENABLED          | Whether Ficon_Tin_Tir_Emulation is enabled on that tunnel.    | smallint |      |
| FICON_DEVICE_LEVEL_ACK_EMULATION_ENABLED | Whether Device_Level_Ack_Emulation is enabled on that tunnel. | smallint |      |
| FICON_TAPE_WRITE_MAX_PIPE                | The value for this on the tunnel.                             | int      |      |
| FICON_TAPE_READ_MAX_PIPE                 | The value for this on the tunnel.                             | int      |      |
| FICON_TAPE_WRITE_MAX_OPS                 | The value for this on the tunnel.                             | int      |      |
| FICON_TAPE_READ_MAX_OPS                  | The value for this on the tunnel.                             | int      |      |
| FICON_TAPE_WRITE_TIMER                   | The value for this on the tunnel.                             | int      |      |
| FICON_TAPE_MAX_WRITE_CHAIN               | The value for this on the tunnel.                             | int      |      |
| FICON_OXID_BASE                          | The value for this on the tunnel.                             | int      |      |
| FICON_XRC_EMULATION_ENABLED              | Whether XRC Emulation is enabled on the tunnel.               | smallint |      |

**TABLE 111** FCIP\_TUNNEL\_DETAILS (Continued)

| Field                              | Definition                                    | Format   | Size |
|------------------------------------|-----------------------------------------------|----------|------|
| FICON_TAPE_WRITE_EMULATION_ENABLED | Whether this is enabled on that tunnel.       | smallint |      |
| FICON_TAPE_READ_EMULATION_ENABLED  | Whether this is enabled on that tunnel.       | smallint |      |
| FICON_DEBUG_FLAGS                  | FICON_DEBUG_FLAGS for that particular tunnel. | double   |      |

## FCIP Tunnel Stats

**TABLE 112** FCIP\_TUNNEL\_STATS

| Field            | Definition                                        | Format           | Size |
|------------------|---------------------------------------------------|------------------|------|
| ID*              |                                                   | int              |      |
| TUNNEL_DBID      | References the ID in FCIP_TUNNEL table.           | int              |      |
| SWITCH ID        | References the ID in CORE_SWITCH table.           | int              |      |
| CREATION TIME    | The polling time.                                 | timestamp        |      |
| TX               | Transmit (TX) value in bytes.                     | double precision |      |
| RX               | Receive (RX) value in bytes.                      | double precision |      |
| TX_UTILIZATION   | Transmit utilization value in percentage.         | double precision |      |
| RX_UTILIZATION   | Receive utilization value in percentage.          | double precision |      |
| DROPPED PACKETS  | The number of dropped packets.                    | double precision |      |
| COMPRESSION      | The compression value.                            | double precision |      |
| LATENCY          | The latency value.                                | double precision |      |
| LINK_RETRANSMITS | The number of link retransmits.                   | double precision |      |
| ACTIVE_STATE     | State of collection:<br>0 = failed<br>1 = success | smallint         |      |

**TABLE 113** FCIP\_TUNNEL\_STATS\_30MIN

| Field          | Definition | Format           | Size |
|----------------|------------|------------------|------|
| ID*            |            | int              |      |
| TUNNEL_DBID    |            | int              |      |
| SWITCH ID      |            | int              |      |
| CREATION TIME  |            | timestamp        |      |
| TX             |            | double precision |      |
| RX             |            | double precision |      |
| TX_UTILIZATION |            | double precision |      |
| RX_UTILIZATION |            | double precision |      |

**TABLE 113** FCIP\_TUNNEL\_STATS\_30MIN (Continued)

| Field            | Definition | Format           | Size |
|------------------|------------|------------------|------|
| DROPPED PACKETS  |            | double precision |      |
| COMPRESSION      |            | double precision |      |
| LATENCY          |            | double precision |      |
| LINK_RETRANSMITS |            | double precision |      |
| ACTIVE_STATE     |            | smallint         |      |

**TABLE 114** FCIP\_TUNNEL\_STATS\_2HOUR

| Field            | Definition | Format           | Size |
|------------------|------------|------------------|------|
| ID*              |            | int              |      |
| TUNNEL_DBID      |            | int              |      |
| SWITCH ID        |            | int              |      |
| CREATION TIME    |            | timestamp        |      |
| TX               |            | double precision |      |
| RX               |            | double precision |      |
| TX_UTILIZATION   |            | double precision |      |
| RX_UTILIZATION   |            | double precision |      |
| DROPPED PACKETS  |            | double precision |      |
| COMPRESSION      |            | double precision |      |
| LATENCY          |            | double precision |      |
| LINK_RETRANSMITS |            | double precision |      |
| ACTIVE_STATE     |            | smallint         |      |

**TABLE 115** FCIP\_TUNNEL\_STATS\_1DAY

| Field           | Definition | Format           | Size |
|-----------------|------------|------------------|------|
| ID*             |            | int              |      |
| TUNNEL_DBID     |            | int              |      |
| SWITCH ID       |            | int              |      |
| CREATION TIME   |            | timestamp        |      |
| TX              |            | double precision |      |
| RX              |            | double precision |      |
| TX_UTILIZATION  |            | double precision |      |
| RX_UTILIZATION  |            | double precision |      |
| DROPPED PACKETS |            | double precision |      |
| COMPRESSION     |            | double precision |      |
| LATENCY         |            | double precision |      |

**TABLE 115** FCIP\_TUNNEL\_STATS\_1DAY (Continued)

| Field            | Definition | Format           | Size |
|------------------|------------|------------------|------|
| LINK_RETRANSMITS |            | double precision |      |
| ACTIVE_STATE     |            | smallint         |      |

**TABLE 116** FCIP\_TUNNEL

| Field                      | Definition                                   | Format   | Size |
|----------------------------|----------------------------------------------|----------|------|
| ID*                        |                                              | int      |      |
| ETHERNET_PORT_ID           | GigE Port ID on which the tunnel is created. | int      |      |
| TUNNEL_ID                  | Tunnel ID for that GigE Port.                | smallint |      |
| VLAN_TAG                   | VLAN Tag on the tunnel (if present).         | int      |      |
| SOURCE_IP                  | Source IP on which the tunnel is created.    | char     | 64   |
| DEST_IP                    | Destination IP on the other end of tunnel.   | char     | 64   |
| LOCAL_WWN                  | Local port WWN for the tunnel.               | char     | 23   |
| REMOTE_WWN_RESTRICT        | Remote Port WWN for the tunnel.              | char     | 23   |
| COMMUNICATION_RATE         | Bandwidth specified for the tunnel.          | double   |      |
| MIN_RETRANSMIT_TIME        | FCIP Tunnel Parameter.                       | int      |      |
| SELECTIVE_ACK_ENABLED      | FCIP Tunnel Parameter.                       | smallint |      |
| KEEP_ALIVE_TIMEOUT         | FCIP Tunnel Parameter.                       | int      |      |
| MAX_RETRANSMISSION         | FCIP Tunnel Parameter.                       | int      |      |
| PATH_MTU_DISCOVERY_ENABLED | FCIP Tunnel Parameter.                       | smallint |      |
| WAN_TOV_ENABLED            | FCIP Tunnel Parameter.                       | smallint |      |
| TUNNEL_STATUS              | Tunnel Status (Active/Inactive).             | int      |      |

## GigE Port Stats

**TABLE 117** GIGE\_PORT\_STATS

| Field          | Definition                                      | Format           | Size |
|----------------|-------------------------------------------------|------------------|------|
| ID*            |                                                 | int              |      |
| SWITCH_ID      | References the ID in CORE_SWITCH table.         | int              |      |
| PORT_ID        | References the ID in SWITCH_PORT table.         | int              |      |
| CREATION_TIME  | The polling time.                               | timestamp        |      |
| TX             | Transmit (TX) value in bytes.                   | double precision |      |
| RX             | Receive (RX) value in bytes.                    | double precision |      |
| TX_UTILIZATION | Transmit utilization (TX%) value in percentage. | double precision |      |
| RX_UTILIZATION | Receive utilization (RX%) value in percentage.  | double precision |      |

**TABLE 117** GIGE\_PORT\_STATS (Continued)

| Field           | Definition                 | Format           | Size |
|-----------------|----------------------------|------------------|------|
| DROPPED PACKETS | Number of dropped packets. | double precision |      |
| COMPRESSION     | The compression value.     | double precision |      |
| LATENCY         | The latency value.         | double precision |      |
| BANDWIDTH       | The bandwidth value.       | double precision |      |

**TABLE 118** GIGE\_PORT\_STATS\_30MIN

| Field           | Definition | Format           | Size |
|-----------------|------------|------------------|------|
| ID*             |            | int              |      |
| SWITCH ID       |            | int              |      |
| PORT_ID         |            | int              |      |
| CREATION TIME   |            | timestamp        |      |
| TX              |            | double precision |      |
| RX              |            | double precision |      |
| TX_UTILIZATION  |            | double precision |      |
| RX_UTILIZATION  |            | double precision |      |
| DROPPED PACKETS |            | double precision |      |
| COMPRESSION     |            | double precision |      |
| LATENCY         |            | double precision |      |
| BANDWIDTH       |            | double precision |      |

**TABLE 119** GIGE\_PORT\_STATS\_2HOUR

| Field           | Definition | Format           | Size |
|-----------------|------------|------------------|------|
| ID*             |            | int              |      |
| SWITCH ID       |            | int              |      |
| PORT_ID         |            | int              |      |
| CREATION TIME   |            | timestamp        |      |
| TX              |            | double precision |      |
| RX              |            | double precision |      |
| TX_UTILIZATION  |            | double precision |      |
| RX_UTILIZATION  |            | double precision |      |
| DROPPED PACKETS |            | double precision |      |
| COMPRESSION     |            | double precision |      |
| LATENCY         |            | double precision |      |
| BANDWIDTH       |            | double precision |      |

**TABLE 120** GIGE\_PORT\_STATS\_1DAY

| Field           | Definition | Format           | Size |
|-----------------|------------|------------------|------|
| ID*             |            | int              |      |
| SWITCH ID       |            | int              |      |
| PORT_ID         |            | int              |      |
| CREATION TIME   |            | timestamp        |      |
| TX              |            | double precision |      |
| RX              |            | double precision |      |
| TX_UTILIZATION  |            | double precision |      |
| RX_UTILIZATION  |            | double precision |      |
| DROPPED PACKETS |            | double precision |      |
| COMPRESSION     |            | double precision |      |
| LATENCY         |            | double precision |      |
| BANDWIDTH       |            | double precision |      |

## ISL

**TABLE 121** ISL\_INFO

| Name                   | Source                     |
|------------------------|----------------------------|
| ID                     | ISL.ID                     |
| FABRIC_ID              | ISL.FABRIC_ID              |
| COST                   | ISL.COST                   |
| TYPE                   | ISL.TYPE                   |
| SOURCE_DOAMIN_ID       | ISL.SOURCE_DOMAIN_ID       |
| SOURCE PORT NUMBER     | ISL.SOURCE_PORT_NUMBER     |
| SOURCE SWITCH ID       | SOURCE_VIRTUAL_SWITCH.ID   |
| SOURCE SWITCH NAME     | SOURCE_VIRTUAL_SWITCH.NAME |
| SOURCE SWITCH PORT ID  | SOURCE_SWITCH_PORT.ID      |
| SOURCE SWITCH PORT WWN | SOURCE_SWITCH_PORT.WWN     |
| DEST DOMAIN ID         | ISL.DEST_DOMAIN_ID         |
| DEST PORT NUMBER       | ISL.DEST_PORT_NUMBER       |
| DEST SWITCH ID         | DEST_VIRTUAL_SWITCH.ID     |
| DEST SWITCH NAME       | DEST_VIRTUAL_SWITCH.NAME   |
| DEST SWITCH PORT ID    | DEST_SWITCH_PORT.ID        |
| DEST SWITCH PORT WWN   | DEST_SWITCH_PORT.WWN       |

**TABLE 122** ISL\_TRUNK\_INFO

| Name                     | Source                          |
|--------------------------|---------------------------------|
| ID                       | ISL_TRUNK_GROUP.ID              |
| COST                     | ISL_INFO.COST                   |
| TYPE                     | ISL_INFO.TYPE                   |
| SOURCE PORT NUMBER       | ISL_INFO.SOURCE_PORT_NUMBER     |
| SOURCE SWITCH ID         | ISL_INFO.SOURCE_SWITCH_ID       |
| SOURCE SWITCH IP ADDRESS | SOURCE_CORE_SWITCH.IP_ADDRESS   |
| SOURCE SWITCH WWN        | SOURCE_VIRTUAL_SWITCH.WWN       |
| MASTER PORT              | ISL_INFO.SOURCE_DOMAIN_ID       |
| SOURCE SWITCH NAME       | ISL_INFO.SOURCE_SWITCH_NAME     |
| SOURCE SWITCH PORT ID    | ISL_INFO.SOURCE_SWITCH_PORT_ID  |
| DEST PORT NUMBER         | ISL_INFO.DEST_PORT_NUMBER       |
| DEST SWITCH ID           | ISL_INFO.DEST_SWITCH_ID         |
| DEST SWITCH IP ADDRESS   | DEST_CORE_SWITCH.IP_ADDRESS     |
| DEST SWITCH WWN          | DEST_VIRTUAL_SWITCH.WWN         |
| DEST SWITCH PORT WWN     | ISL_INFO.SOURCE_SWITCH_PORT_WWN |
| SOURCE SWITCH PORT WWN   |                                 |
| REMOTE MASTER PORT       |                                 |
| DEST SWITCH NAME         | ISL_INFO.DEST_SWITCH_NAME       |
| DEST SWITCH PORT ID      | ISL_INFO.DEST_SWITCH_PORT_ID    |

**TABLE 123** ISL

| Field              | Definition                                   | Format    | Size |
|--------------------|----------------------------------------------|-----------|------|
| ID*                |                                              | int       |      |
| FABRIC_ID          | Fabric DB ID.                                | int       |      |
| SOURCE_DOMAIN_ID   | Source domain ID.                            | int       |      |
| SOURCE_PORT_NUMBER | Source port number.                          | smallint  |      |
| DEST_DOMAIN_ID     | Destination domain ID.                       | int       |      |
| DEST_PORT_NUMBER   | Destination port number.                     | smallint  |      |
| COST               | The cost of the link.                        | int       |      |
| TYPE               | The type of link.                            | smallint  |      |
| TRUSTED            | 1 = ISL is trusted<br>0 = ISL is not trusted | smallint  |      |
| CREATION_TIME      | Time at which this record was created.       | timestamp |      |
| MISSING            | 1 = ISL is missing<br>0 = ISL is not missing | smallint  |      |
| MISSING_TIME       | Time at which ISL went missing.              | timestamp |      |

**TABLE 124** FABRIC

| Field                | Definition                                                                          | Format    | Size |
|----------------------|-------------------------------------------------------------------------------------|-----------|------|
| ID*                  |                                                                                     | int       |      |
| SAN_ID               | Foreign key to SAN table; usually 1 since there is only one SAN.                    | int       |      |
| SEED_SWITCH_WWN      | WWN of the virtual switch used as seed switch to discover the fabric.               | char      | 23   |
| NAME                 | User-assigned fabric name.                                                          | varchar   | 256  |
| CONTACT              | User-assigned "contact" for the fabric.                                             | varchar   | 256  |
| LOCATION             | User-assigned "location" for the fabric.                                            | varchar   | 256  |
| DESCRIPTION          | User-assigned fabric description.                                                   | varchar   | 256  |
| TYPE                 | Type of fabric:<br>0 = legacy fabric<br>1 = base fabric<br>2 = logical fabric       | smallint  |      |
| SECURE               | 1 = it is a secured fabric.                                                         | smallint  |      |
| AD_ENVIRONMENT       | 1 = there are user-defined ADs in this fabric.                                      | smallint  |      |
| MANAGED              | 1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric. | smallint  |      |
| MANAGEMENT_STATE     | Bit map to indicate various management indications for the fabric.                  | smallint  |      |
| TRACK_CHANGES        | 1 = changes (member switches, ISL and devices) in the fabric are tracked.           | smallint  |      |
| STATS_COLLECTION     | 1 = statistics collection is enabled on the fabric.                                 | smallint  |      |
| CREATION_TIME        | When the fabric record is inserted, i.e., created.                                  | timestamp |      |
| LAST_FABRIC_CHANGED  | Time when fabric last changed.                                                      | timestamp |      |
| LAST_SCAN_TIME       |                                                                                     | timestamp |      |
| LAST_UPDATE_TIME     | Time when fabric was last updated.                                                  | timestamp |      |
| ACTIVE_ZONESET_NAME  | Name of the zone set which is effective / active in that fabric.                    | varchar   | 256  |
| USER_DEFINED_VALUE_1 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_2 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_3 | User-defined custom value.                                                          | varchar   | 256  |

**TABLE 125** ISL\_TRUNK\_MEMBER

| Field        | Definition                  | Format   | Size |
|--------------|-----------------------------|----------|------|
| GROUP_ID*    | ISL_TRUNK_GROUP DB ID.      | int      |      |
| PORT_NUMBER* | Port number of member port. | smallint |      |

**TABLE 126** ISL\_TRUNK\_GROUP

| Field             | Definition                  | Format   | Size |
|-------------------|-----------------------------|----------|------|
| ID*               |                             | int      |      |
| VIRTUAL_SWITCH_ID | Virtual switch DB ID.       | int      |      |
| MASTER_USER_PORT  | Port number of master port. | smallint |      |

## License

**TABLE 127** LICENSE\_FEATURE\_MAP

| Field       | Definition                                                      | Format  | Size |
|-------------|-----------------------------------------------------------------|---------|------|
| LICENSE_ID* | Foreign Key (SWITCH_LICENSE.ID) and is part of the primary key. | integer |      |
| FEATURE_ID* | Foreign Key (LICENSED_FEATURE.ID) and is part of the primary.   | integer |      |

**TABLE 128** LICENSED\_FEATURE

| Field       | Definition                                               | Format  | Size |
|-------------|----------------------------------------------------------|---------|------|
| ID*         |                                                          | int     |      |
| NAME        | License feature name, a short text description.          | varchar | 64   |
| DESCRIPTION | Optional detailed description about the license feature. | varchar | 256  |

**TABLE 129** SWITCH\_LICENSE

| Field          | Definition                                       | Format  | Size |
|----------------|--------------------------------------------------|---------|------|
| ID*            |                                                  | int     |      |
| CORE_SWITCH_ID | Refers to the entry in the CORE_SWITCH table.    | int     |      |
| LICENSE_KEY    | Stores the license key obtained from the switch. | varchar | 256  |

**TABLE 130** CORE\_SWITCH

| Field | Definition | Format | Size |
|-------|------------|--------|------|
| ID*   |            | int    |      |

## Encryption Device

**TABLE 131** KEY VAULT

| Field              | Definition                                                                                                   | Format   | Size |
|--------------------|--------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                |                                                                                                              | int      |      |
| IP_ADDRESS         | The IP Address (IPv4, IPv6, or hostname) of the key vault.                                                   | varchar  | 512  |
| PORT_NUMBER        | The TCP port number for the key vault.                                                                       | int      |      |
| PUBLIC_CERTIFICATE | The key vault's public key certificate. Switches use this to establish a secure connection to the key vault. | varchar  | 4096 |
| CRETIFICATE_LABEL  | A text name to identify the certificate.                                                                     | varchar  | 64   |
| POSITION           | Whether this key vault is the primary key vault or the backup key vault:<br>0 = primary<br>1 = backup        | smallint |      |

**TABLE 132** CRYPTO\_SWITCH

| Field                     | Definition                                                                                                                                                                                                        | Format   | Size |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| SWITCH_ID*                | Primary key. The value is the same as the primary key of a record in the VIRTUAL_SWITCH table                                                                                                                     | int      |      |
| ENCRYPTION_GROUP_ID       | Foreign key to the ENCRYPTION_GROUP table. Identifies the Encryption Group that this switch belongs to. Null indicates the switch is not part of an Encryption Group.                                             | int      |      |
| GROUP_LEADER_POSITION     | No longer used. Previously indicated whether this switch is the group leader. Use GROUP_LEADER_ID in the ENCRYPTION_GROUP table instead.                                                                          | smallint |      |
| TAPE_ENCRYPTION           | No longer used. Previously enabled or disabled tape encryption at the switch level. This feature has been removed from Fabric OS.                                                                                 | smallint |      |
| TAPE_KEY_POLICY           | No longer used. Previously used to configure a separate data encryption key per volume or per group. This feature has been removed from Fabric OS.                                                                | smallint |      |
| PRIMARY_VAULT_LINK_STATUS | The status of the link key for the primary key vault. Link keys are used only for NetApp LKM key vaults. For possible values, see the enum definition in the DTO class.                                           | smallint |      |
| BACKUP_VAULT_LINK_STATUS  | The status of the link key for the backup key vault. Link keys are used only for NetApp LKM key vaults. For possible values, see the enum definition in the DTO class.                                            | smallint |      |
| CP_CERTIFICATE            | The public key certificate, in PEM format, of the switch's Control Processor module. This certificate is exchanged with other switches to establish secure communication between switches in an Encryption Group. | varchar  | 4096 |

**TABLE 132** CRYPTO\_SWITCH

| Field                             | Definition                                                                                                                                                                                                 | Format   | Size |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| KAC_CERTIFICATE                   | The public key certificate, in PEM format, of the switch's Key Archive Client module. This certificate is installed on key vaults to establish secure communication between this switch and the key vault. | varchar  | 4096 |
| PRIMARY_VAULT_CONNECTIVITY_STATUS | The status of the network connection between this switch and the primary key vault. For possible values, see the enum definition in the DTO class.                                                         | smallint |      |
| BACKUP_VAULT_CONNECTIVITY_STATUS  | The status of the network connection between this switch and the backup key vault. For possible values, see the enum definition in the DTO class.                                                          | smallint |      |

**TABLE 133** ENCRYPTION GROUP

| Field                | Definition                                                                                                                                                                                                                                                                                                                                                                                                                              | Format   | Size |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                  |                                                                                                                                                                                                                                                                                                                                                                                                                                         | int      |      |
| NAME                 | User-assigned name for this encryption group.                                                                                                                                                                                                                                                                                                                                                                                           | varchar  | 64   |
| LEADER_SWITCH_ID     | Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that currently provides central configuration and reporting capabilities for the encryption group. This column may be null if the group leader is not in a discovered fabric.                                                                                            | int      |      |
| LEADER_SWITCH_WWN    | The Node WWN of the current group leader switch. Each encryption group has one group leader switch.                                                                                                                                                                                                                                                                                                                                     | char     | 23   |
| DEPLOYMENT_MODE      | Indicates Transparent (0) or Non Transparent (1) deployment mode. Only Transparent mode is currently supported. All switches in the Encryption Group share the same deployment mode. Transparent mode uses re-direction zones to preserve existing zoning of physical hosts and targets. Non-transparent mode requires zoning changes to zone physical hosts with Virtual Targets and to zone Virtual Initiators with physical targets. | smallint |      |
| FAILBACK_MODE        | Indicates Automatic (0) or Manual (1) failback. Failback occurs when a previously unavailable Encryption Engine comes back online. In Auto mode, the restored EncryptionEngine resumes encrypting all traffic for target containers configured on the Encryption Engine. In manual mode, encryption continues running on the backup encryption engines until manually changed.                                                          | smallint |      |
| SYSTEM_CARD_REQUIRED | Boolean value that indicates whether a System Card (smart card) must be inserted in the Encryption Engine to enable the engine after power-up. This feature is not yet supported.                                                                                                                                                                                                                                                       | smallint |      |

**TABLE 133** ENCRYPTION GROUP

| Field                        | Definition                                                                                                                                                                                                                                                     | Format   | Size |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ACTIVE_MASTER_KEY_STAT<br>US | The operational status of the "master key" or "Key Encryption Key (KEK)" used to encrypt Data Encryption Keys in a key vault. Not used for NetApp LKM key vaults.<br>0 = not used<br>1 = required but not present<br>2 = present but not backed up<br>3 = okay | smallint |      |
| ALT_MASTER_KEY_STATUS        | The operational status of an alternate "master key" used to access older data encryption keys. Not used for NetApp LKM key vaults.<br>0 = not used<br>1 = not present<br>3 = okay                                                                              | smallint |      |
| QUORUM_SIZE                  | The number of authentication cards required to approve certain secure operations. This feature is not yet supported.                                                                                                                                           | smallint |      |
| RECOVERY_SET_SIZE            | No longer used. Previously used to indicate the number of smart cards used to back up a Master Key. The number of cards is now specified when the backup is created, and not persisted in the database.                                                        | smallint |      |
| KEY_VAULT_TYPE               | Indicates the type of key vault used by switches in this Encryption Group.<br>0 = NetApp Lifetime Key Manager (LKM)<br>1 = RSA Key Manager (RKM)<br>2 = Internal key storage (for demo use only)                                                               | smallint |      |
| PRIMARY_KEY_VAULT_ID         | Foreign key reference to the KEY_VAULT record that describes the primary key vault for this Encryption Group. Null if no primary key vault is configured.                                                                                                      | int      |      |
| BACKUP_KEY_VAULT_ID          | Foreign key reference to the KEY_VAULT record that describes the backup key vault for this Encryption Group. Null if no backup key vault is configured.                                                                                                        | int      |      |
| GROUP_LEADER_STATUS          | Stores the status of the Group leader node                                                                                                                                                                                                                     | int      |      |

**TABLE 134** ENCRYPTION\_TAPE\_POOL

| Field                | Definition                                                                                                                                     | Format | Size |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------|------|
| ID*                  |                                                                                                                                                | int    |      |
| SWITCH_ID            | No longer used. Tape pools used to belong to specific switches, but are now shared by all switches in an encryption group.                     | int    |      |
| ENCRYPTION_ENGINE_ID | No longer used. Tape pools used to belong to specific encryption engines, but are now shared by all encryption engines in an encryption group. | int    |      |
| ENCRYPTION_GROUP_ID  | Foreign key reference to the ENCRYPTION_GROUP record that describes which Encryption Group this tape pool belongs to.                          | int    |      |

**TABLE 134** ENCRYPTION\_TAPE\_POOL

| Field                    | Definition                                                                                                                                                                                                                         | Format   | Size |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| TAPE_POOL_NAME           | User-supplied name or number for the tape pool. This is the same name or number specified in the tape backup application. Numbers are stored in hex.                                                                               | varchar  | 64   |
| TAPE_POOL_OPERATION_MODE | Specifies which type of encryption should be used by tape volumes in this tape pool.<br>0 = Native<br>1 = DF-compatible.                                                                                                           | smallint |      |
| TAPE_POOL_POLICY         | Specifies whether tape volumes in this tape pool should be encrypted.<br>0 = encrypted<br>1 = cleartext                                                                                                                            | smallint |      |
| KEY_EXPIRATION           | Number of days each data encryption key for this tape pool should be used. After the configured number of days, a new data encryption key is automatically generated for any further tape volumes in this pool. 0 = no expiration. | int      |      |
| TAPE_POOL_LABEL_TYPE     | Indicates whether the TAPE_POOL_NAME field is a name or a number.<br>0 = name<br>1 = number                                                                                                                                        | smallint |      |

**TABLE 135** RECOVERY\_CARD\_GROUP\_MAPPING

| Field               | Definition                                                                                              | Format | Size |
|---------------------|---------------------------------------------------------------------------------------------------------|--------|------|
| ID*                 |                                                                                                         | int    |      |
| ENCRYPTION_GROUP_ID | Foreign key reference to the ENCRYPTION_GROUP for which a recovery card is registered.                  | int    |      |
| SMART_CARD_ID       | Foreign key reference to the SMART_CARD that is registered as a recovery card for the encryption group. | int    |      |
| POSITION            | The position of the card within the recovery card set.<br>1 = first card, 2 = second card, etc.         | int    |      |

**TABLE 136** ENCRYPTION\_GROUP\_MEMBER

| Field               | Definition                                                                                                                                     | Format   | Size |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                 |                                                                                                                                                | int      |      |
| ENCRYPTION_GROUP_ID | Foreign key reference to the ENCRYPTION_GROUP record that identifies the encryption group that this member switch belongs to.                  | int      |      |
| MEMBER_IP_ADDRESS   | The management IP address (IPv4, IPv6, or hostname) of the member switch.                                                                      | varchar  | 128  |
| MEMBER_WWN          | The Node WWN of the member switch.                                                                                                             | char     | 23   |
| MEMBER_STATUS       | The reachability status of the member switch as seen by the group leader switch. For possible values see the enum definition in the DTO class. | smallint |      |

**TABLE 137** QUORUM\_CARD\_GROUP\_MAPPING

| Field               | Definition                                                                                                    | Format | Size |
|---------------------|---------------------------------------------------------------------------------------------------------------|--------|------|
| ID                  |                                                                                                               | int    |      |
| ENCRYPTION_GROUP_ID | Foreign key reference to the ENCRYPTION_GROUP for which an authorization card is registered.                  | int    |      |
| SMART_CARD_ID       | Foreign key reference to the SMART_CARD that is registered as an authorization card for the encryption group. | int    |      |

**TABLE 138** HA CLUSTER

| Field               | Definition                                                                                                                                                                                                                               | Format  | Size |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|
| ID*                 |                                                                                                                                                                                                                                          | int     |      |
| NAME                | User-supplied name for the HA Cluster.                                                                                                                                                                                                   | varchar | 64   |
| ENCRYPTION_GROUP_ID | Foreign key reference to the ENCRYPTION_GROUP that contains this HA Cluster.                                                                                                                                                             | int     |      |
| MEMBER_LIST         | A comma-separated list of Encryption Engines in the HA Cluster. Each engine is identified by a switch node WWN, followed by a slash (/), followed by the slot number. The slot number is 0 if the switch does not have removable blades. | varchar | 256  |

**TABLE 139** SMART CARD

| Field              | Definition                                                                                                                                             | Format   | Size |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                |                                                                                                                                                        | int      |      |
| CARD_TYPE          | Indicates how this smart card is configured: 0 = authorization card.                                                                                   | smallint |      |
| CARD_INFO          | Additional smart card details. For recovery set cards, the details include the recovery set size and the card's position within the set; e.g., 2 of 5. |          |      |
| CARDCN_ID          | A unique name for the card, derived from the card's serial number and usage.                                                                           | varchar  | 64   |
| FIRST_NAME         | Optional first name of the person responsible for this card.                                                                                           | varchar  | 64   |
| LAST_NAME          | Optional last name of the person responsible for this card.                                                                                            | varchar  | 64   |
| NOTES              | User-supplied notes about the card.                                                                                                                    | varchar  | 256  |
| PUBLIC_CERTIFICATE | The public key certificate of the card, in PEM format. Used to validate the card and set up a secure communications channel to the card.               | varchar  | 4096 |
| CERTIFICATE_LABEL  | User-supplied name for the card's public key certificate.                                                                                              | varchar  | 64   |

**TABLE 139** SMART CARD

| Field         | Definition                                                                                                                                               | Format    | Size |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| GROUP_NAME    | The name of the Encryption Group used to initialize the card. For recovery set cards, this identifies which group's master key is backed up on the card. | varchar   | 64   |
| CREATION_TIME | The date and time that the card was initialized. For recovery set cards, this is the date and time the master key was written to the card.               | timestamp | 256  |

**TABLE 140** ENCRYPTION ENGINE

| Field               | Definition                                                                                                                                                                                           | Format   | Size |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                 |                                                                                                                                                                                                      | int      |      |
| SWITCH_ID           | Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that contains this encryption engine. | int      |      |
| SLOT_NUMBER         | For chassis switches, the slot or blade that contains the encryption engine. Always 0 for switches with a single embedded encryption engine.                                                         | smallint | 64   |
| STATUS              | Not used. Previously used to indicate the engine's operational status. Replaced by EE_STATE.                                                                                                         | smallint | 64   |
| HA_CLUSTER_ID       | Foreign key reference to an HA_CLUSTER record. Identifies the HA Cluster that this engine belongs to. Null if this engine does not belong to an HA Cluster.                                          | int      | 64   |
| SYSTEM_CARD_ID      | Foreign key reference to the SMART_CARD record that identifies the System Card required to enable this engine. Null if no System Card has been registered yet. This feature is not yet supported.    | int      | 256  |
| SYSTEM_CARD_STATUS  | Indicates whether a System Card is currently inserted in the Encryption Engine, and whether the card is valid or not. This feature is not yet supported.                                             | smallint | 4096 |
| WWN_POOLS_AVAILABLE | Not used. Previously used to indicate the number of WWN pools remaining for allocation on this encryption engine. This feature is no longer supported.                                               | int      | 64   |
| STATE               | Administrative state for this engine:<br>0 = disabled<br>1 = enabled                                                                                                                                 | smallint | 64   |
| SP_CERTIFICATE      | The public key certificate, in PEM format, for the Security Processor within the Encryption Engine. Used to create link keys for NetApp LKM key vaults.                                              | varchar  | 4096 |
| EE_STATE            | The operational status of this Encryption Engine. For possible values, see the enum definition in the DTO class.                                                                                     | int      |      |

## Encryption Container

**TABLE 141** CRYPTO HOST

| Field                      | Definition                                                                    | Format | Size |
|----------------------------|-------------------------------------------------------------------------------|--------|------|
| ID*                        |                                                                               | int    |      |
| CRYPTO_TARGET_CONTAINER_ID | Foreign key reference to the CRYPTO_TARGET_CONTAINER that contains this host. | int    |      |
| VI_NODE_WWN                | Node WWN of Virtual Initiator that represents this host.                      | char   | 23   |
| VI_PORT_WWN                | Port WWN of Virtual Initiator that represents this host.                      | char   | 23   |
| HOST_PORT_WWN              | Physical (real) host's Port WWN                                               | char   | 23   |
| HOST_NODE_WWN              | Physical (real) host's Node WWN                                               | char   | 23   |

**TABLE 142** CRYPTO TARGET CONTAINER

| Field                | Definition                                                                                                                                                                                        | Format   | Size |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                  |                                                                                                                                                                                                   | int      |      |
| ENCRYPTION_ENGINE_ID | Foreign key reference to the ENCRYPTION_ENGINE that owns this container.                                                                                                                          | int      |      |
| NAME                 | A user-supplied name for the container.                                                                                                                                                           | varchar  | 64   |
| VT_NODE_WWN          | The Node WWN of the Virtual Target that represents the real physical target device.                                                                                                               | char     | 23   |
| VT_PORT_WWN          | The Port WWN of the Virtual Target that represents the real physical target device.                                                                                                               | char     | 23   |
| FAILOVER_STATUS      | Indicates whether this container's target is being encrypted by the encryption engine on which the container is configured (value 0) or by another encryption engine in the HA Cluster (value 1). | smallint |      |
| DEVICE_STATUS        | The physical target storage device operational status when the virtual initiator last attempted to access the target. For possible values, see the enum definition in the DTO class.              | smallint |      |
| DEVICE_TYPE          | Indicates whether the target storage device is a disk (0) or tape (1) device.                                                                                                                     | smallint |      |
| TARGET_PORT_WWN      | The Port WWN of the physical target storage device associated with this container.                                                                                                                | char     | 23   |
| TARGET_NODE_WWN      | The Node WWN of the physical target storage device associated with this container                                                                                                                 | char     | 23   |

**TABLE 143** CRYPTO LUN

| Field                      | Definition                                                                                                                                                                                                                                              | Format    | Size |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| ID*                        |                                                                                                                                                                                                                                                         | int       |      |
| CRYPTO_TARGET_CONTAINER_ID | Foreign key reference to the CRYPTO_TARGET_CONTAINER that contains the host for which these LUNs are configured.                                                                                                                                        | int       |      |
| SERIAL_NUMBER              | The LUN serial number, used to identify the physical LUN.                                                                                                                                                                                               | varchar   | 64   |
| ENCRYPTION_STATE           | Boolean. True (1) if LUN is being encrypted. False (0) if cleartext.                                                                                                                                                                                    | smallint  |      |
| STATUS                     | Not currently used but left in for possible future use. Replaced by LUN_STATE.                                                                                                                                                                          | smallint  |      |
| REKEY_INTERVAL             | The number of days that data encryption keys should be used before automatically generating a new key. 0 = infinite, i.e., no re-keying.                                                                                                                | int       |      |
| VOLUME_LABEL_PREFIX        | A user-configured string used to construct the Brocade-specific volume label on encrypted tapes. Ignored for disk LUNs.                                                                                                                                 | varchar   | 256  |
| LAST_REKEY_DATE            | The last time a data encryption key was generated for this LUN. REKEY_INTERVAL days after this date, a new key will be generated.                                                                                                                       | timestamp |      |
| LAST_REKEY_STATUS          | The success or failure of the most recent re-keying operation, if any. This field is not currently used, but is left in the hope that Fabric OS will support it in the future. Only valid for disk LUNs.                                                | smallint  |      |
| LAST_REKEY_PROGRESS        | Indicates whether a re-key operation is in progress. 0 = no re-keying in progress. > 0 = percentage done of re-keying operation in progress. Only valid for disk LUNs.                                                                                  | smallint  |      |
| CURRENT_VOLUME_LABEL       | If a tape session is in progress, this is the volume label for the currently mounted tape. Only valid for tape LUNs.                                                                                                                                    | varchar   | 2048 |
| PRIOR_ENCRYPTION_STATE     | Not used. When configuring a new disk LUN, this field indicates whether the LUN is already encrypted (1) or cleartext (0). This information does not need to be persisted. Only valid for disk LUNs.                                                    | smallint  |      |
| ENCRYPTION_FORMAT          | If ENCRYPTION_STATE is true, ENCRYPTION_FORMAT indicates the type of encryption. 0 = cleartext, 1 = DF-compatible, 2 = native.                                                                                                                          | smallint  |      |
| ENCRYPT_EXISTING_DATA      | Not used. When configuring a disk LUN that was previously cleartext and is to be encrypted, this property tells the switch whether or not to start a re-keying operation to encrypt the existing LUN data. This property does not need to be persisted. | smallint  |      |

**TABLE 143** CRYPTO LUN

| Field                 | Definition                                                                                                                                                                                                                                                                                                  | Format   | Size |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| DECRYPT_EXISTING_DATA | Not used. When configuring disk LUN that was previously encrypted and is to become cleartext, this property tells the switch whether or not to start a re-keying operation to decrypt the existing LUN data. This property does not need to be persisted. This feature is no longer supported in Fabric OS. | smallint |      |
| KEY_ID                | Hex-encoded binary key vault ID for the current data encryption key for this LUN. This ID may be used to locate the data encryption key in the key vault                                                                                                                                                    | varchar  | 64   |
| CRYPTO_HOST_ID        | Foreign key reference to the CRYPTO_HOST that uses this LUN.                                                                                                                                                                                                                                                | int      |      |
| LUN_NUMBER            | The Logical Unit Number of the LUN, as seen by the LUNs host. This may be an integer (0 - 65565) or a WWN-format 8-byte hex number.                                                                                                                                                                         | varchar  | 23   |
| BLOCK_SIZE            | The LUN's Logical Block Size, in bytes. Only valid for disk LUNs.                                                                                                                                                                                                                                           | int      |      |
| TOTAL_BLOCKS          | The total number of logical blocks in the LUN. Multiplying BLOCK_SIZE by TOTAL_BLOCKS gives the LUN size in bytes.                                                                                                                                                                                          | int      |      |
| LUN_STATE             | LUN operational status, such as OK or disabled for various reasons. For possible values see the enum definition in CryptoClientConstants.                                                                                                                                                                   | int      |      |
| LUN_FLAGS             | Bitmap of LUN options. The only option currently used is bit 0 (least significant) which indicates that the LUN must be manually enabled because it has been disabled due to inconsistent metadata detected.                                                                                                | bigint   |      |

**TABLE 144** ENCRYPTION ENGINE

| Field          | Definition                                                                                                                                                                                           | Format   | Size |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*            |                                                                                                                                                                                                      | int      |      |
| SWITCH_ID      | Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that contains this encryption engine. | int      |      |
| SLOT_NUMBER    | For chassis switches, the slot or blade that contains the encryption engine. Always 0 for switches with a single embedded encryption engine.                                                         | smallint |      |
| STATUS         | Not used. Previously used to indicate the engine's operational status. Replaced by EE_STATE.                                                                                                         | smallint |      |
| HA_CLUSTER_ID  | Foreign key reference to an HA_CLUSTER record. Identifies the HA Cluster that this engine belongs to. Null if this engine does not belong to an HA Cluster.                                          | int      |      |
| SYSTEM_CARD_ID | Foreign key reference to the SMART_CARD record that identifies the System Card required to enable this engine. Null if no System Card has been registered yet. This feature is not yet supported.    | int      |      |

**TABLE 144** ENCRYPTION ENGINE

| Field               | Definition                                                                                                                                               | Format   | Size |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| SYSTEM_CARD_STATUS  | Indicates whether a System Card is currently inserted in the Encryption Engine, and whether the card is valid or not. This feature is not yet supported. | smallint |      |
| WWN_POOLS_AVAILABLE | Not used. Previously used to indicate the number of WWN pools remaining for allocation on this encryption engine. This feature is no longer supported.   | int      |      |
| STATE               | Administrative state for this engine:<br>0 = disabled<br>1 = enabled                                                                                     | smallint |      |
| SP_CERTIFICATE      | The public key certificate, in PEM format, for the Security Processor within the Encryption Engine. Used to create link keys for NetApp LKM key vaults.  | varchar  | 4096 |
| EE_STATE            | The operational status of this Encryption Engine. For possible values, see the enum definition in the DTO class.                                         | int      |      |

**TABLE 145**

| Name                     | Source                                                |
|--------------------------|-------------------------------------------------------|
| TARGET_CONTAINER_ID      | CRYPTO_TARGET_CONTAINER.ID TARGET_CONTAINER_ID        |
| NAME                     | CRYPTO_TARGET_CONTAINER.NAME                          |
| VT_NODE_WWN              | CRYPTO_TARGET_CONTAINER.VT_NODE_WWN                   |
| VT_PORT_WWN              | CRYPTO_TARGET_CONTAINER.VT_PORT_WWN                   |
| FAILOVER_STATUS          | CRYPTO_TARGET_CONTAINER.FAILOVER_STATUS               |
| DEVICE_STATUS            | CRYPTO_TARGET_CONTAINER.DEVICE_STATUS                 |
| DEVICE_TYPE              | CRYPTO_TARGET_CONTAINER.DEVICE_TYPE                   |
| TARGET_PORT_WWN          | CRYPTO_TARGET_CONTAINER.TARGET_PORT_WWN               |
| TARGET_NODE_WWN          | CRYPTO_TARGET_CONTAINER.TARGET_NODE_WWN               |
| ENCRYPTION ENGINE STATUS | ENCRYPTION_ENGINE.STATUS ENCRYPTION_ENGINE_STATUS     |
| HA_CLUSTER_ID            | ENCRYPTION_ENGINE.HA_CLUSTER_ID                       |
| SYSTEM_CARD_ID           | ENCRYPTION_ENGINE.SYSTEM_CARD_ID                      |
| SYSTEM_CARD_STATUS       | ENCRYPTION_ENGINE.SYSTEM_CARD_STATUS                  |
| WWN_POOLS_AVAILABLE      | ENCRYPTION_ENGINE.WWN_POOLS_AVAILABLE                 |
| ENCRYPTION ENGINE STATE  | ENCRYPTION_ENGINE.STATE ENCRYPTION_ENGINE_STATE       |
| ENCRYPTION ENGINE ID     | ENCRYPTION_ENGINE.ID ENCRYPTION_ENGINE_ID             |
| SWITCH_ID                | CRYPTO_SWITCH.SWITCH_ID SWITCH_ID                     |
| ENCRYPTION_GROUP_ID      | CRYPTO_SWITCH.ENCRYPTION_GROUP_ID ENCRYPTION_GROUP_ID |

**TABLE 146**

| <b>Name</b>                | <b>Source</b>                  |
|----------------------------|--------------------------------|
| CRYPTO HOST ID             | LUN.CRYPTO_HOST_ID             |
| CRYPTO LUN ID              | LUN.ID CRYPTO_LUN_ID           |
| LUN NUMBER                 | LUN.LUN_NUMBER                 |
| CRYPTO TARGET CONTAINER ID | LUN.CRYPTO_TARGET_CONTAINER_ID |
| SERIAL NUMBER              | LUN.SERIAL_NUMBER              |
| ENCRYPTION STATE           | LUN.ENCRYPTION_STATE           |
| STATUS                     | LUN.STATUS                     |
| REKEY_INTERVAL             | LUN.REKEY_INTERVAL             |
| VOLUME_LABEL_PREFIX        | LUN.VOLUME_LABEL_PREFIX        |
| LAST_REKEY_DATE            | LUN.LAST_REKEY_DATE            |
| LAST_REKEY_STATUS          | LUN.LAST_REKEY_STATUS          |
| LAST_REKEY_PROGRESS        | LUN.LAST_REKEY_PROGRESS        |
| CURRENT_VOLUME_LABEL       | LUN.CURRENT_VOLUME_LABEL       |
| PRIOR_ENCRYPTION_STATE     | LUN.PRIOR_ENCRYPTION_STATE     |
| ENCRYPTION_FORMAT          | LUN.ENCRYPTION_FORMAT          |
| ENCRYPT_EXISTING_DATA      | LUN.ENCRYPT_EXISTING_DATA      |
| DECRYPT_EXISTING_DATA      | LUN.DECRYPT_EXISTING_DATA      |
| KEY_ID                     | LUN.KEY_ID                     |
| BLOCK_SIZE                 | LUN.BLOCK_SIZE                 |
| TOTAL_BLOCKS               | LUN.TOTAL_BLOCKS               |
| LUN_STATE                  | LUN.LUN_STATE                  |
| LUN_FLAGS                  | LUN.LUN_FLAGS                  |
| HOST_PORT_WWN              | CRYPTO_HOST.HOST_PORT_WWN      |
| HOST_NODE_WWN              | CRYPTO_HOST.HOST_NODE_WWN      |

## Meta SAN

**TABLE 147** LSAN\_DEVICE

| Field           | Definition                          | Format | Size |
|-----------------|-------------------------------------|--------|------|
| ID*             |                                     | int    |      |
| BB_FABRIC_ID    | Backbone fabric DB ID.              | int    |      |
| FCR_FABRIC_ID   | FID assigned to edge fabric.        | int    |      |
| DEVICE_PORT_WWN | Device port WWN of physical device. | char   | 23   |
| PHYSICAL_PID    | PID of physical device.             | char   | 6    |

**TABLE 148** LSAN\_PROXY\_DEVICE

| Field           | Definition                   | Format  | Size |
|-----------------|------------------------------|---------|------|
| FCR_FABRIC_ID*  | FID assigned to edge fabric  | int     |      |
| PROXY_PID*      | Proxy device PID             | char    | 6    |
| STATE           | State of the device          | varchar | 128  |
| LSAN_DEVICE_ID* | LSAN_DEVICE record reference | int     |      |

**TABLE 149** FCR\_ROUTE

| Field         | Definition                   | Format  | Size |
|---------------|------------------------------|---------|------|
| ID*           |                              | INT     |      |
| BB_FABRIC_ID  | Backbone fabric DB ID.       | INT     |      |
| FCR_FABRIC_ID | FID assigned to edge fabric. | INT     |      |
| SWITCH_WWN    | WWN of the router switch.    | VARCHAR | 128  |
| NR_PORT_ID    | Route parameter.             | INT     |      |
| FCRP_COST     | Route parameter.             | INT     |      |
| EX_PORT_WWN   | Ex_port WWN.                 | VARCHAR | 128  |

**TABLE 150** FABRIC

| Field           | Definition                                                            | Format  | Size |
|-----------------|-----------------------------------------------------------------------|---------|------|
| ID*             |                                                                       | int     |      |
| SAN_ID          | Foreign key to SAN table; usually 1 since there is only one SAN.      | int     |      |
| SEED_SWITCH_WWN | WWN of the virtual switch used as seed switch to discover the fabric. | char    | 23   |
| NAME            | User-assigned fabric name.                                            | varchar | 256  |
| CONTACT         | User-assigned "contact" for the fabric.                               | varchar | 256  |
| LOCATION        | User-assigned "location" for the fabric.                              | varchar | 256  |
| DESCRIPTION     | User-assigned fabric description.                                     | varchar | 256  |

**TABLE 150** FABRIC (Continued)

| Field                | Definition                                                                          | Format    | Size |
|----------------------|-------------------------------------------------------------------------------------|-----------|------|
| TYPE                 | Type of fabric:<br>0 = legacy fabric<br>1 = base fabric<br>2 = logical fabric       | smallint  |      |
| SECURE               | 1 = it is a secured fabric.                                                         | smallint  |      |
| AD_ENVIRONMENT       | 1 = there are user-defined ADs in this fabric.                                      | smallint  |      |
| MANAGED              | 1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric. | smallint  |      |
| MANAGEMENT_STATE     | Bit map to indicate various management indications for the fabric.                  | smallint  |      |
| TRACK_CHANGES        | 1 = changes (member switches, ISL and devices) in the fabric are tracked.           | smallint  |      |
| STATS_COLLECTION     | 1 = statistics collection is enabled on the fabric.                                 | smallint  |      |
| CREATION_TIME        | When the fabric record is inserted, i.e., created.                                  | timestamp |      |
| LAST_FABRIC_CHANGED  | Time when fabric last changed.                                                      | timestamp |      |
| LAST_SCAN_TIME       |                                                                                     | timestamp |      |
| LAST_UPDATE_TIME     | Time when fabric was last updated.                                                  | timestamp |      |
| ACTIVE_ZONESET_NAME  | Name of the zone set which is effective / active in that fabric.                    | varchar   | 256  |
| USER_DEFINED_VALUE_1 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_2 | User-defined custom value.                                                          | varchar   | 256  |
| USER_DEFINED_VALUE_3 | User-defined custom value.                                                          | varchar   | 256  |

**TABLE 151** IFL

| Field          | Definition                | Format   | Size |
|----------------|---------------------------|----------|------|
| ID*            |                           | int      |      |
| EDGE_FABRIC_ID | Edge Fabric ID.           | int      |      |
| EDGE_PORT_WWN  | Edge Fabric Port WWN.     | varchar  | 128  |
| BB_FABRIC_ID   | Backbone Fabric ID.       | int      |      |
| BB_PORT_WWN    | Backbone Fabric Port WWN. | varchar  | 128  |
| BB_RA_TOV      | Backbone RA TOV.          | int      |      |
| BB_ED_TOV      | Backbone ED TOV.          | int      |      |
| BB_PID_FORMAT  | Backbone PID Format.      | smallint |      |

**TABLE 152** IFL\_INFO

| Name             | Source                        |
|------------------|-------------------------------|
| ID               | IFL.ID                        |
| EDGE_FABRIC_ID   | IFL.EDGE_FABRIC_ID            |
| FCR SWITCH ID    | FCR_PORT.VIRTUAL_SWITCH_ID    |
| EDGE_PORT_WWN    | IFL.EDGE_PORT_WWN             |
| BB_FABRIC_ID     | IFL.BB_FABRIC_ID              |
| BB_PORT_WWN      | IFL.BB_PORT_WWN               |
| BB_RA_TOV        | IFL.BB_RA_TOV                 |
| BB_ED_TOV        | IFL.BB_ED_TOV                 |
| BB_PID_FORMAT    | IFL.BB_PID_FORMAT             |
| EDGE SWITCH ID   | SWITCH_PORT.VIRTUAL_SWITCH_ID |
| EDGE PORT ID     | SWITCH_PORT.ID                |
| EDGE PORT NUMBER | SWITCH_PORT.USER_PORT_NUMBER  |
| EDGE PORT TYPE   | SWITCH_PORT.TYPE              |

## Network

**TABLE 153** IP\_INTERFACE

| Field            | Definition                      | Format | Size |
|------------------|---------------------------------|--------|------|
| ID*              |                                 | int    |      |
| ETHERNET_PORT_ID | GigE Port ID.                   | int    |      |
| IP_ADDRESS       | IP address on the Ip_interface. | vchar  | 64   |
| NET_MASK         | Subnet mask for the interface.  | vchar  | 64   |
| MTU_SIZE         | MTU Size for that interface.    | int    |      |
| CHECKSUM         | Check Sum.                      | vchar  | 64   |

**TABLE 154** IP\_ROUTE

| Field            | Definition                                         | Format | Size |
|------------------|----------------------------------------------------|--------|------|
| ID*              |                                                    | int    |      |
| ETHERNET_PORT_ID | GigE Port ID.                                      | int    |      |
| PORT_NUMBER      | Port Number related to the GigE Port.              | int    |      |
| SLOT_NUMBER      | Slot Number related to the GigE Port.              | int    |      |
| NET_MASK         | Subnet Mask for the Route.                         | vchar  | 64   |
| GATEWAY          | Gateway for the Route.                             | vchar  | 64   |
| IP_ADDRESS       | IP Address created after "&" operation of gateway. | vchar  | 64   |
| METRIC           | Metric.                                            | int    |      |

**TABLE 154** IP\_ROUTE (Continued)

| Field    | Definition | Format  | Size |
|----------|------------|---------|------|
| FLAG     | Flag.      | int     |      |
| CHECKSUM | Check Sum. | varchar | 64   |

## Others

**TABLE 155** SYSTEM\_PROPERTY

| Field | Definition                  | Format  | Size |
|-------|-----------------------------|---------|------|
| NAME* | The name of the property.   | char    | 64   |
| VALUE | The value for the property. | VARCHAR | 2048 |

**TABLE 156** OUI\_VENDOR

| Field  | Definition                                                                    | Format  | Size |
|--------|-------------------------------------------------------------------------------|---------|------|
| OUI*   | Vendor OUI, 6-digit hexadecimal number which can have leading digits as zero. | char    | 6    |
| VENDOR | Vendor name.                                                                  | varchar | 64   |

**TABLE 157** OUI\_GUESSED\_DEVICE\_MAP

| Field | Definition                           | Format  | Size |
|-------|--------------------------------------|---------|------|
| OUI*  | Vendor OUI.                          | char    | 6    |
| TYPE  | Guessed device type for this vendor. | varchar | 32   |

**TABLE 158** FEATURE

| Field       | Definition                                | Format  | Size |
|-------------|-------------------------------------------|---------|------|
| FEATURE_ID* | ID used to uniquely identify the feature. | int     | 6    |
| NAME        | Name of the feature.                      | varchar | 256  |
| DESCRIPTION | Description for the feature.              | varchar | 256  |

**TABLE 159** FEATURE\_EDITION\_MAP

| Field        | Definition                                                        | Format | Size |
|--------------|-------------------------------------------------------------------|--------|------|
| FEATURE_ID*  | ID used to uniquely identify the feature.                         | int    |      |
| EDITION_MASK | Used to associate a feature to the edition (Reserved for future). | int    |      |

## Port Fencing

**TABLE 160** PORT\_FENCING\_POLICY

| Field                | Definition                                                                                                                                                                                                                                                    | Format   | Size |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                  |                                                                                                                                                                                                                                                               | int      |      |
| NAME                 | Name of the policy. The length of the field should be 62 because M-EOS switch supports only maximum 62 characters.                                                                                                                                            | varchar  | 62   |
| TYPE                 | 0 = ISL Protocol<br>1 = Link<br>2 = Security                                                                                                                                                                                                                  | smallint |      |
| THRESHOLD_LIMIT      | Threshold Limits for M-EOS Switch.                                                                                                                                                                                                                            | int      |      |
| THRESHOLD_DURATION   | Duration In minutes for M-EOS Switch.                                                                                                                                                                                                                         | int      |      |
| DEFAULT_POLICY       | 1 = the default port fencing policies.<br>0 = the non-default policies.<br>The default port fencing policies are:<br>For ISL - Default Protocol Error Policy<br>For Link Violation type - Default Link Level Policy<br>For Security - Default Security Policy | smallint |      |
| B_THRESHOLD_LIMIT    | Threshold Limits for Fabric OS Switch (Not Supported).                                                                                                                                                                                                        | int      |      |
| B_THRESHOLD_DURATION | Duration in minutes for Fabric OS Switch (Not Supported).                                                                                                                                                                                                     | int      |      |

**TABLE 161** PORT\_FENCING\_POLICY\_MAP

| Field       | Definition                                                                                            | Format   | Size |
|-------------|-------------------------------------------------------------------------------------------------------|----------|------|
| ID*         |                                                                                                       | int      |      |
| POLICY_ID   | Foreign key to ID column of PORT_FENCING_POLICY table.                                                | int      |      |
| LEVEL       | 0 = All Fabric<br>1 = Fabric<br>2 = Core Switch Group<br>3 = Switch<br>4 = Port Type<br>5 = Port List | smallint |      |
| SUB_LEVEL   | 1 = E_Port<br>2 = F_Port<br>3 = FL_Port, Fabric WWN, Switch WWN                                       | char     | 23   |
| NODE        | WWN of Node which policy assigned.                                                                    | char     | 23   |
| INHERITANCE | Directly assigned or inherited from root level.<br>0 = Directly assigned<br>1 = Indirectly assigned   | smallint |      |

## Quartz

**TABLE 162** QRTZ\_JOB\_DETAILS

| Field             | Definition                                                                                                                    | Format  | Size |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------|---------|------|
| JOB_NAME*         | Name of the job.                                                                                                              | varchar | 80   |
| JOB_GROUP*        | Name of the job group.                                                                                                        | varchar | 80   |
| DESCRIPTION       | Description of the job (optional).                                                                                            | varchar | 120  |
| JOB_CLASS_NAME    | The instance of the job that will be executed.                                                                                | varchar | 128  |
| IS_DURABLE        | Whether the job should remain stored after it is orphaned.                                                                    | bit     |      |
| IS_VOLATILE       | Whether the job should not be persisted in the JobStore for re-use after program restarts.                                    | bit     |      |
| IS_STATEFUL       | Whether the job implements the interface StatefulJob.                                                                         | bit     |      |
| REQUESTS_RECOVERY | Instructs the scheduler whether or not the job should be re-executed if a "recovery" or "fail-over" situation is encountered. | bit     |      |
| JOB_DATA          | To persist the job-related and application-related informations.                                                              | image   |      |

**TABLE 163** QRTZ\_TRIGGERS

| Field          | Definition                                                                                                                                                     | Format   | Size |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| TRIGGER_NAME*  | Name of the trigger.                                                                                                                                           | varchar  | 80   |
| TRIGGER_GROUP* | Name of the trigger group.                                                                                                                                     | varchar  | 80   |
| JOB_NAME       | Name of the job.                                                                                                                                               | varchar  | 80   |
| JOB_GROUP      | Name of the job group.                                                                                                                                         | varchar  | 80   |
| IS_VOLATILE    | Whether the trigger should be persisted in the JobStore for re-use after program restarts.                                                                     | bit      |      |
| DESCRIPTION    | A description for the trigger instance - may be useful for remembering/displaying the purpose of the trigger, though the description has no meaning to Quartz. | varchar  | 120  |
| NEXT_FIRE_TIME | The next fire time in milliseconds.                                                                                                                            | numeric  | 13,0 |
| PREV_FIRE_TIME | The previous fired time in milliseconds.                                                                                                                       | numeric  | 13,0 |
| TRIGGER_STATE  | The state of the trigger (viz. Error, wait,etc.)                                                                                                               | varchar  | 16   |
| TRIGGER_TYPE   | The type of the trigger (Simple,cron).                                                                                                                         | varchar  | 8    |
| START_TIME     | The job start time.                                                                                                                                            | numeric  | 13,0 |
| END_TIME       | The job end time (-1 means infinite).                                                                                                                          | numeric  | 13,0 |
| CALENDAR_NAME  |                                                                                                                                                                | varchar  | 80   |
| MISFIRE_INSTR  | Instructs the scheduler to execute the misfired job.                                                                                                           | smallint |      |
| JOB_DATA       | Persists the job-related info.                                                                                                                                 | image    |      |

**TABLE 164** QRTZ\_SIMPLE\_TRIGGERS

| Field           | Definition                                      | Format  | size |
|-----------------|-------------------------------------------------|---------|------|
| TRIGGER_NAME*   | Name of the trigger                             | varchar | 80   |
| TRIGGER_GROUP*  | name of the trigger group                       | varchar | 80   |
| REPEAT_COUNT    | number of times to repeat                       | numeric | 13,0 |
| REPEAT_INTERVAL | interval for first and second job               | numeric | 13,0 |
| TIMES_TRIGGERED | Number of times the corresponding trigger fired | numeric | 13,0 |

**TABLE 165** QRTZ\_FIRED\_TRIGGERS

| Field             | Definition                                                                                     | Format  | size |
|-------------------|------------------------------------------------------------------------------------------------|---------|------|
| ENTRY_ID*         | Fired instance ID.                                                                             | varchar | 95   |
| TRIGGER_NAME      | Name of the trigger.                                                                           | varchar | 80   |
| TRIGGER_GROUP     | Name of the trigger group.                                                                     | varchar | 80   |
| IS_VOLATILE       | Whether the job should not be persisted in the JobStore for re-use after the program restarts. | bit     |      |
| INSTANCE_NAME     | Trigger instance name.                                                                         | varchar | 80   |
| FIRED_TIME        | The trigger fired time.                                                                        | numeric | 13,0 |
| STATE             | The fired trigger job state.                                                                   | varchar | 16   |
| JOB_NAME          | Name of the job.                                                                               | varchar | 80   |
| JOB_GROUP         | Name of the job group.                                                                         | varchar | 80   |
| IS_STATEFUL       | Whether the job implements the interface StatefulJob.                                          | bit     |      |
| REQUESTS_RECOVERY | True or false.                                                                                 | bit     |      |

**TABLE 166** QRTZ\_JOB\_LISTENERS

| Field         | Definition                          | Format  | Size |
|---------------|-------------------------------------|---------|------|
| JOB_NAME*     | Name of the job.                    | varchar | 80   |
| JOB_GROUP*    | Name of the job group.              | varchar | 80   |
| JOB_LISTENER* | Job listener action class instance. | varchar | 80   |

**TABLE 167** QRTZ\_CRON\_TRIGGERS

| Field           | Definition                                                                               | Format  | Size |
|-----------------|------------------------------------------------------------------------------------------|---------|------|
| TRIGGER_NAME*   | Name of the trigger.                                                                     | varchar | 80   |
| TRIGGER_GROUP*  | Name of the trigger group.                                                               | varchar | 80   |
| CRON_EXPRESSION | The CRON trigger Expression (ex:"0 0 12 * * ?" - meaning:Fire at 12pm (noon) every day). | varchar | 80   |
| TIME_ZONE_ID    | Given "cron" expression resolved with respect to the TimeZone.                           | varchar | 80   |

**TABLE 168** QRTZ\_JTRIGGER\_LISTENERS

| Field             | Definition                 | Format  | Size |
|-------------------|----------------------------|---------|------|
| TRIGGER_NAME*     | Name of the trigger.       | varchar | 80   |
| TRIGGER_GROUP*    | Name of the trigger group. | varchar | 80   |
| TRIGGER_LISTENER* | The listener action.       | varchar | 80   |

**TABLE 169** QRTZ\_BLOB\_TRIGGERS

| Field          | Definition                 | Format  | Size |
|----------------|----------------------------|---------|------|
| TRIGGER_NAME*  | Name of the trigger.       | varchar | 80   |
| TRIGGER_GROUP* | Name of the trigger group. | varchar | 80   |
| BLOB_DATA      | The Scheduler info.        | varchar | 80   |

**TABLE 170** QRTZ\_SCHEDULER\_STATE

| Field             | Definition                       | Format  | Size |
|-------------------|----------------------------------|---------|------|
| INSTANCE_NAME*    | Instance of the scheduler.       | varchar | 80   |
| LAST_CHECKIN_TIME | Last fired time in milliseconds. | numeric | 13,0 |
| CHECKIN_INTERVAL  | Repeat interval.                 | numeric | 13,0 |
| RECOVERER         | Misfire instruction.             | varchar | 80   |

**TABLE 171** QRTZ\_LOCKS

| Field      | Definition                                     | Format  | Size |
|------------|------------------------------------------------|---------|------|
| LOCK_NAME* | Resource identification name assigned by user. | varchar | 40   |

**TABLE 172** QRTZ\_CALENDARS

| Field          | Definition            | Format  | Size |
|----------------|-----------------------|---------|------|
| CALENDAR_NAME* | Name of the Calendar. | varchar | 80   |
| CALENDAR       | Calendar object.      | image   |      |

**TABLE 173** QRTZ\_PAUSED\_TRIGGER\_GRP

| Field          | Definition                 | Format  | Size |
|----------------|----------------------------|---------|------|
| TRIGGER_GROUP* | Name of the trigger group. | varchar | 80   |

## Reports

**TABLE 174** REPORT\_TYPE

| Field       | Definition                       | Format  | Size |
|-------------|----------------------------------|---------|------|
| ID*         | Meta Data for available reports. | int     |      |
| NAME        | Report name.                     | varchar | 128  |
| DESCRIPTION | Report type description.         | varchar | 256  |

**TABLE 175** GENERATED\_REPORT

| Field         | Definition                                                     | Format    | Size |
|---------------|----------------------------------------------------------------|-----------|------|
| ID*           |                                                                | int       |      |
| NAME          | Report name.                                                   | varchar   | 256  |
| TYPE_ID       | Report type.                                                   | int       |      |
| EFCM_USER     | The Management application user who has generated this report. | varchar   | 128  |
| REPORT_OBJECT | Report object BLOB.                                            | image     |      |
| TIMESTAMP_    | Timestamp when the report is generated.                        | timestamp |      |

## Role Based Access Control

**TABLE 176** USER\_ROLE\_MAP

| Field      | Definition                             | Format  | Size |
|------------|----------------------------------------|---------|------|
| USER_NAME* | User name.                             | varchar | 128  |
| ROLE_ID*   | Role ID, which is mapped for the user. | int     |      |

**TABLE 177** ROLE

| Field       | Definition        | Format  | Size |
|-------------|-------------------|---------|------|
| ID*         |                   | int     |      |
| NAME        | Role name.        | varchar | 128  |
| DESCRIPTION | Role description. | varchar | 512  |

**TABLE 178** ROLE\_PRIVILEGE\_MAP

| Field         | Definition                                                    | Format   | Size |
|---------------|---------------------------------------------------------------|----------|------|
| ROLE_ID*      | User role ID.                                                 | int      |      |
| PRIVILEGE_ID* | Privilege ID.                                                 | int      |      |
| PERMISSION    | Privilege permission:<br>1 = RO<br>2 = RW<br>0 = No privilege | smallint |      |

**TABLE 179** PRIVILEGE

| Field | Definition      | Format  | Size |
|-------|-----------------|---------|------|
| ID*   |                 | int     |      |
| NAME  | Privilege Name. | varchar | 128  |

**TABLE 180** PRIVILEGE\_GROUP\_MAP

| Field         | Definition          | Format | Size |
|---------------|---------------------|--------|------|
| GROUP_ID*     | Privilege group ID. | int    |      |
| PRIVILEGE_ID* | Privilege ID.       | int    | 128  |

**TABLE 181** PRIVILEGE\_GROUP

| Field | Definition            | Format  | Size |
|-------|-----------------------|---------|------|
| ID*   |                       | int     |      |
| NAME  | Privilege group name. | varchar | 128  |

**TABLE 182** ROLE\_PRIVILEGE\_INFO

| name             | Source                        |
|------------------|-------------------------------|
| ID               | ROLE.ID                       |
| ROLE NAME        | ROLE.NAME                     |
| ROLE DESCRIPTION | ROLE.DESCRPTION               |
| ID               | PRIVILEGE.ID                  |
| NAME             | PRIVILEGE.NAME                |
| PERMISSION       | ROLE_PRIVILEGE_MAP.PERMISSION |

**TABLE 183** USER\_

| Field                | Definition                    | Format   | Size |
|----------------------|-------------------------------|----------|------|
| NAME*                | User name.                    | varchar  | 128  |
| DESCRIPTION          | User description.             | varchar  | 512  |
| PASSWORD             | User password.                | varchar  | 512  |
| EMAIL                | User e-mail ID.               | varchar  | 1024 |
| NOTIFICATION_ENABLED | Flag for e-mail notification. | smallint |      |

**TABLE 184** USER\_RESOURCE\_MAP

| Field              | Definition                                         | Format  | Size |
|--------------------|----------------------------------------------------|---------|------|
| USER_NAME*         | User name.                                         | varchar | 128  |
| RESOURCE_GROUP_ID* | Resource group name, which is mapped for the user. | int     |      |

**TABLE 185** RESOURCE\_GROUP

| Field       | Definition                  | Format  | Size |
|-------------|-----------------------------|---------|------|
| ID*         |                             | int     |      |
| NAME        | Resource group name.        | varchar | 128  |
| DESCRIPTION | Resource group description. | varchar | 512  |

**TABLE 186** RESOURCE\_FABRIC\_MAP

| Field              | Definition                                 | Format | Size |
|--------------------|--------------------------------------------|--------|------|
| RESOURCE_GROUP_ID* | Resource group ID.                         | int    |      |
| FABRIC_ID*         | Fabric ID, which is in the resource group. | int    |      |

**TABLE 187** USER\_ROLE\_RESOURCE\_INFO

| name                | Source                                  |
|---------------------|-----------------------------------------|
| RESOURCE GROUP ID   | RESOURCE_GROUP.ID RESOURCE_GROUP_ID     |
| RESOURCE GROUP NAME | RESOURCE_GROUP.NAME RESOURCE_GROUP_NAME |
| ROLE ID             | ROLE.ID ROLE_ID                         |
| ROLE NAME           | ROLE.NAME ROLE_NAME                     |
| NAME                | USER_.NAME USER_NAME                    |

## SNMP

**TABLE 188** SNMP\_CREDENTIALS

| Field                  | Definition                                                                                                                                                                                                                                                                                                                          | Format   | Size |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*                    |                                                                                                                                                                                                                                                                                                                                     | int      |      |
| VIRTUAL_SWITCH_ID      | Virtual switch ID for which this instance of the SNMP credentials apply.                                                                                                                                                                                                                                                            | int      |      |
| RECIPIENT_ID           | Recipient in the MESSAGE_RECIPIENT table.                                                                                                                                                                                                                                                                                           | int      |      |
| POR)_NUMBER            | Port number of the SNMP agent on the switch for get and set requests.                                                                                                                                                                                                                                                               | smallint |      |
| RETRY_COUNT            | Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.                                                                                                                                                                                                                                        | smallint |      |
| TIMEOUT                | Timeout value in seconds for a get/set request to the SNMP agent. Default value is 5.                                                                                                                                                                                                                                               | smallint |      |
| VERSION                | SNMP agent version running on the switch, as in SNMPv1 or SNMPv3.                                                                                                                                                                                                                                                                   | vchar    | 6    |
| READ_COMMUNITY_STRING  | The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to a device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.                                                                                   | vchar    | 64   |
| WRITE_COMMUNITY_STRING | The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to a device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1.                                                                                 | vchar    | 64   |
| USER_NAME              | A human readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                                                                                                      | vchar    | 64   |
| CONTEXT_NAME           | Text ID associated with the user, used by the SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                                                                            | vchar    | 128  |
| AUTH_PROTOCOL          | An indication of whether messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. The supported values for this field are: usmNoAuthProtocol, usmHMACMD5AuthProtocol, and usmHMACSHAAuthProtocol. This is applicable if the agent is configured to operate in SNMPv3. | vchar    | 16   |
| AUTH_PASSWORD          | The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                                                                       | vchar    | 64   |

**TABLE 188** SNMP\_CREDENTIALS (Continued)

| Field         | Definition                                                                                                                                                                                                                                                                                | Format  | Size |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|
| PRIV_PROTOCOL | An indication of whether messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. The current values for this field are: usmNoPrivProtocol and usmDESPrivProtocol. This is applicable if the agent is configured to operate in SNMPv3. | varchar | 16   |
| PRIV_PASSWORD | The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                         | varchar | 64   |

**TABLE 189** SNMP\_PROFILE

| Field                  | Definition                                                                                                                                                                                                                                         | Format   | Size |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| NAME*                  | A text string representing a set of SNMP agent profile. When created, one or more virtual switches could refer to this profile for its SNMP credentials unless a unique set of SNMP credentials has been defined in SNMP_CREDENTIAL.               | varchar  | 256  |
| PORT_NUMBER            | Port number of the SNMP agent on the switch for get and set requests                                                                                                                                                                               | smallint |      |
| RETRY_COUNT            | Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.                                                                                                                                                       | smallint |      |
| TIMEOUT                | Timeout value in seconds before for a get/set request to the SNMP agent. Default value is 5.                                                                                                                                                       | smallint |      |
| VERSION                | SNMP agent version running on the switch as in SNMPv1 and SNMPv3                                                                                                                                                                                   | varchar  | 6    |
| READ_COMMUNITY_STRING  | The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.    | varchar  | 64   |
| WRITE_COMMUNITY_STRING | The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to a device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1 | varchar  | 64   |
| USER_NAME              | A human-readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                     | varchar  | 64   |
| CONTEXT_NAME           | A text ID associated with the user, used by SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.                                                                                             | varchar  | 128  |

**TABLE 189** SNMP\_PROFILE (Continued)

| Field         | Definition                                                                                                                                                                                                                                                                                                                                 | Format  | Size |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|
| AUTH_PROTOCOL | An indication of whether or not messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. The supported values for this field are: usmNoAuthProtocol, usmHMACMD5AuthProtocol, and usmHMACSHAAuthProtocol. This is applicable if the agent is configured to operate in SNMPv3. | varchar | 16   |
| AUTH_PASSWORD | The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                                                                              | varchar | 64   |
| PRIV_PROTOCOL | An indication of whether or not messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. The current values for this field are: usmNoPrivProtocol and usmDESPrivProtocol. This is applicable if the agent is configured to operate in SNMPv3.                                           | varchar | 16   |
| PRIV_PASSWORD | The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.                                                                                                                                                                          | varchar | 64   |

**TABLE 190** SNMP\_V3\_FORWARDING\_CREDENTIAL

| Field         | Definition              | Format  | Size |
|---------------|-------------------------|---------|------|
| ID*           |                         | int     |      |
| USER_NAME     | USM user name.          | varchar | 64   |
| CONTEXT_NAME  | USM context name.       | VARCHAR | 128  |
| AUTH_PROTOCOL | Authorization protocol. | VARCHA  | 16   |
| AUTH_PASSWORD | Authorization password. | VARCHAR | 64   |
| PRIV_PROTOCOL | Privilege protocol.     | VARCHAR | 16   |
| PRIV_PASSWORD | Privilege password.     | VARCHAR | 64   |

## Stats

**TABLE 191** FAVORITES

| Field              | Definition                                                                                                                                                                                                      | Format    | Size |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| ID*                |                                                                                                                                                                                                                 | int       |      |
| NAME               | Name of the favorite.                                                                                                                                                                                           | varchar   | 64   |
| USER_              | The application user credentials.                                                                                                                                                                               | varchar   | 128  |
| TOP_N              | The top number of ports(5,10,15,20).                                                                                                                                                                            | varchar   | 40   |
| SELECTION_FILTER   | Types of ports (FC/FCIP/GE) and End-to-End Monitors.                                                                                                                                                            | varchar   | 40   |
| FROM_TIME          | The time interval in which the graph is shown. Time interval can be predefined or custom. If FROM_TIME is Custom, the user can choose the number of minutes/hours/days or specify the time interval.            | varchar   | 40   |
| CUSTOM_LAST_VALUE  | The number of minutes/hours/days. It becomes null in two cases.<br>1. When the value of FROM_TIME is not Custom.<br>2. When FROM_TIME is Custom, and user chooses the time interval (CUSTOM_FROM and CUSTOM_TO) | int       |      |
| CUSTOM_TIME_UNIT   | The unit type (Minutes, Hours, Days) of the CUSTOM_LAST_VALUE.                                                                                                                                                  | varchar   | 40   |
| CUSTOM_FROM        | The starting time.                                                                                                                                                                                              | timestamp |      |
| CUSTOM_TO          | The ending time.                                                                                                                                                                                                | timestamp |      |
| GRANULARITY        | The granularity.                                                                                                                                                                                                | varchar   | 40   |
| THRESHOLD          | The reference line.                                                                                                                                                                                             | int       |      |
| MAIN_MEASURE       | The measure of FC/FCIP/GE.                                                                                                                                                                                      | varchar   | 40   |
| ADDITIONAL_MEASURE | The additional measures.                                                                                                                                                                                        | int       |      |

**TABLE 192** USER\_

| Field                | Definition                    | Format   | Size |
|----------------------|-------------------------------|----------|------|
| NAME*                | User name.                    | varchar  | 128  |
| DESCRIPTION          | User description.             | varchar  | 512  |
| PASSWORD             | User password.                | varchar  | 512  |
| EMAIL                | User e-mail ID.               | varchar  | 1024 |
| NOTIFICATION_ENABLED | Flag for e-mail notification. | smallint |      |

**TABLE 193** STATS\_AGING

| Field             | Definition                                                    | Format   | Size |
|-------------------|---------------------------------------------------------------|----------|------|
| ID*               |                                                               | int      |      |
| FIVE_MIN_VALUE    | Configured maximum samples value for the five minute table.   | int      |      |
| THIRTY_MIN_VALUE  | Configured maximum samples value for the thirty minute table. | int      |      |
| TWO_HR_VALUE      | Configured maximum samples value for the two hour table.      | int      |      |
| ONE_DAY_VALUE     | Configured maximum samples value for the one day table.       | int      |      |
| MAX_SAMPLES_VALUE | The maximum number of samples value, i.e., 3456.              | int      |      |
| INTERPOLATE       | Whether interpolation is enabled or disabled.                 | smallint |      |

**TABLE 194** MARCHING\_ANTs

| Field            | Definition                                            | Format | Size |
|------------------|-------------------------------------------------------|--------|------|
| ID*              |                                                       | int    |      |
| THRESHOLD1_VALUE | The marching ants low boundary threshold value (T1).  | int    |      |
| THRESHOLD2_VALUE | The marching ants high boundary threshold value (T2). | int    |      |

**TABLE 195** DEFAULT\_FAVORITES

| Field              | Definition                                                     | Format    | Size |
|--------------------|----------------------------------------------------------------|-----------|------|
| ID                 | Name of the favorite.                                          | int       |      |
| NAME               | The topnumber of ports (5,10,15,20).                           | varchar   | 64   |
| TOP_N              | Types of ports (FC/FCIP/GE) and End-to-End Monitors.           | varchar   | 40   |
| SELECTION_FILTER   | The time interval in which the graph is shown.                 | varchar   | 40   |
| FROM_TIME          | Always null. The default favorite is not customized.           | varchar   | 40   |
| CUSTOM_LAST_VALUE  | Always null. The default favorite is not customized.           | int       |      |
| CUSTOM_TIME_UNIT   | Always null. The default favorite is not customized.           | varchar   | 40   |
| CUSTOM_FROM        | Always null. The default favorite is not customized.           | timestamp |      |
| CUSTOM_TO          | The default five minutes granularity.                          | timestamp |      |
| GRANULARITY        | Always null.                                                   | varchar   | 40   |
| THRESHOLD          | The measure Tx MBps or Rx MBps based on DEFAULT_FAVORITES.NAME | int       |      |
| MAIN_MEASURE       | The Additional measures based on the FAVORITE.MAIN_MEASURE     | varchar   | 40   |
| ADDITIONAL_MEASURE | The Additional measures based on the FAVORITE.MAIN_MEASURE     | int       |      |

## Switch

**TABLE 196** VIRTUAL-SWITCH

| Field                | Definition                                                                         | Format    | Size |
|----------------------|------------------------------------------------------------------------------------|-----------|------|
| ID*                  |                                                                                    | int       |      |
| LOGICAL_ID           | Logical ID of the switch.                                                          | smallint  |      |
| NAME                 | Switch name.                                                                       | varchar   | 64   |
| WWN                  | WWN of the switch.                                                                 | char      | 23   |
| VIRTUAL_FABRIC_ID    | Virtual fabric ID. If VF enabled then will have the VFID; otherwise it will be -1. | smallint  |      |
| DOMAIN_ID            | Domain ID of the switch.                                                           | smallint  |      |
| BASE_SWITCH          | 1 = this is a base switch; otherwise, 0.                                           | smallint  |      |
| SWITCH_MODE          | 2 = switch is in AG mode; otherwise, 0.                                            | smallint  |      |
| ROLE                 | Role of the switch.                                                                | varchar   | 32   |
| FCS_ROLE             | FCS role of the switch.                                                            | varchar   | 16   |
| AD_CAPABLE           | 1 = switch is AD-capable.                                                          | smallint  |      |
| FABRIC_IDID_MODE     | Fabric IDID mode.                                                                  | smallint  |      |
| OPERATIONAL_STATUS   | Operation status of switch.                                                        | varchar   | 128  |
| MAX_ZONE_CONFIG_SIZE | Maximum size of zone configuration on the switch.                                  | int       |      |
| CREATION_TIME        | Time at which this record was created.                                             | timestamp |      |
| LAST_UPDATE_TIME     | Time when this record was last updated.                                            | timestamp |      |
| USER_NAME            | User name of the switch.                                                           | varchar   | 128  |
| PASSWORD             | Password.                                                                          | varchar   | 128  |
| MANAGEMENT_STATE     | Various states as per manageability software like the Management application.      | int       |      |
| STATE                | State of the switch.                                                               | varchar   | 32   |
| STATUS               | Status of the switch.                                                              | varchar   | 32   |
| STATUS_REASON        | Reason for the status.                                                             | varchar   | 2048 |
| USER_DEFINED_VALUE1  |                                                                                    | varchar   | 256  |
| USER_DEFINED_VALUE2  |                                                                                    | varchar   | 256  |
| USER_DEFINED_VALUE3  |                                                                                    | varchar   | 256  |
| CORE_SWITCH_ID       | Core switch DB ID.                                                                 | int       |      |
| INTEROP_MODE         | Mode in which this switch is operating.                                            | smallint  |      |
| CRYPTO_CAPABLE       | 0 = the switch is not crypto-enabled; if capable it will have a non-zero value.    | smallint  |      |
| FCR-CAPABLE          | 0 = the switch is not FCR-enabled; if capable it will have a non-zero value.       | smallint  |      |
| FCIP_CAPABLE         | 0 = the switch is not FCIP-enabled; if capable it will have a non-zero value.      | smallint  |      |

**TABLE 197** CORE\_SWITCH

| Field                | Definition                                                                                                                             | Format    | Size |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| ID*                  |                                                                                                                                        | int       |      |
| IP_ADDRESS           | IP address of the switch.                                                                                                              | varchar   | 128  |
| WWN                  | Chassis WWN.                                                                                                                           | char      | 23   |
| NAME                 | Switch name.                                                                                                                           | varchar   | 64   |
| CONTACT              | Any associated contact name, obtained through SNMP.                                                                                    | varchar   | 256  |
| LOCATION             | Physical location, obtained through SNMP.                                                                                              | varchar   | 256  |
| DESCRIPTION          | User assigned description, obtained through SNMP.                                                                                      | varchar   | 256  |
| TYPE                 | SWBD type number as given by Fabric OS.                                                                                                | smallint  |      |
| MODEL                | Model type of the switch:<br>0 = Unknown<br>1 = Not applicable<br>2 = Fabric OS switch<br>3 = M-EOS switch                             | smallint  |      |
| FIRMWARE_VERSION     | Embedded (Fabric OS or M-EOS) software version.                                                                                        | varchar   | 128  |
| VENDOR               | Switch vendor.                                                                                                                         | varchar   | 256  |
| MAX_VIRTUAL_SWITCHES | Maximum virtual switches allowed on this physical switch.                                                                              | smallint  |      |
| NUM_VIRTUAL_SWITCHES | Actual number of virtual switches carved out of this physical switch. 0 means it is not operating in Virtual Fabric model.             | smallint  |      |
| REACHABLE            | Whether reachable by HTTP.                                                                                                             | smallint  |      |
| UNREACHABLE_TIME     | When the switch became unreachable from HTTP.                                                                                          | timestamp |      |
| OPERATIONAL_STATUS   | Operational status as reported by the embedded software.                                                                               | varchar   | 128  |
| CREATION_TIME        | Time when this record was created by the Management application.                                                                       | timestamp |      |
| LAST_SCAN_TIME       | Time when this record was last updated.                                                                                                | timestamp |      |
| LAST_UPDATE_TIME     | 1 = the Management application server is registered with the switch to receive Syslog.                                                 | timestamp |      |
| SYSLOG_REGISTERED    | 1 = Syslog is enabled for this switch.                                                                                                 | smallint  |      |
| CALL_HOME_ENABLED    | 1 = call home is enabled for this switch.                                                                                              | smallint  |      |
| SNMP_REGISTERED      | 1 = the Management application server is registered with the switch to receive SNMP traps.                                             | smallint  |      |
| USER_IP_ADDRESS      | User-assigned IP address. This is used for M-EOS switches where Fabric OS seed switch fails to get the IP address of the M-EOS switch. | varchar   | 128  |

**TABLE 197** CORE\_SWITCH (Continued)

| Field                      | Definition                                                                                                                                                                                                          | Format  | Size |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------|
| NIC_PROFILE_ID             | NIC profile of the Management application server host used by this switch to communicate in interactive configuration and other operations. It determines which Management application host IP used by this switch. | int     |      |
| MANAGING_SERVER_IP_ADDRESS | IP address of the server which is currently managing this switch. Used for M-EOS switch only. It does not apply to Fabric OS switches.                                                                              | varchar | 128  |

**TABLE 198** NIC\_PROFILE

| Field      | Definition                                                                             | Format  | Size |
|------------|----------------------------------------------------------------------------------------|---------|------|
| ID*        |                                                                                        | int     |      |
| NAME       | The name of the network interface in the format network interface name / host address. | varchar | 255  |
| IP_ADDRESS | The host address of the interface.                                                     | varchar | 128  |

**TABLE 199** SWITCH\_INFO

| name                        | Source                           |
|-----------------------------|----------------------------------|
| PHYSICAL SWITCH ID          | CORE_SWITCH.ID                   |
| PHYSICAL SWITCH NAME        | CORE_SWITCH.NAME                 |
| IP_ADDRESS                  | CORE_SWITCH.IP_ADDRESS           |
| PHYSICAL SWITCH WWN         | CORE_SWITCH.WWN                  |
| PHYSICAL OPERATIONAL STATUS | CORE_SWITCH.OPERATIONAL_STATUS   |
| TYPE                        | CORE_SWITCH.TYPE                 |
| MAX_VIRTUAL_SWITCH          | CORE_SWITCH.MAX_VIRTUAL_SWITCHES |
| NUM)VIRTUAL_SWITCHES        | CORE_SWITCH.NUM_VIRTUAL_SWITCHES |
| FIRMWARE_VERSION            | CORE_SWITCH.FIRMWARE_VERSION     |
| VENDOR                      | CORE_SWITCH.VENDOR               |
| REACHABLE                   | CORE_SWITCH.REACHABLE            |
| UNREACHABLE_TIME            | CORE_SWITCH.UNREACHABLE_TIME     |
| CONTACT                     | CORE_SWITCH.CONTACT              |
| LOCATION                    | CORE_SWITCH.LOCATION             |
| DESCRIPTION                 | CORE_SWITCH.DESCRPTION           |
| MODEL                       | CORE_SWITCH.MODEL                |
| SYSLOG_REGISTERED           | CORE_SWITCH.SYSLOG_REGISTERED    |
| SNMP_REGISTERED             | CORE_SWITCH.SNMP_REGISTERED      |
| CALL_HOME_ENABLED           | CORE_SWITCH.CALL_HOME_ENABLED    |
| USER_IP_ADDRESS             | CORE_SWITCH.USER_IP_ADDRESS      |

**TABLE 199** SWITCH\_INFO

| <b>name</b>                | <b>Source</b>                          |
|----------------------------|----------------------------------------|
| NIC_PROFILE_ID             | CORE_SWITCH.NIC_PROFILE_ID             |
| MANAGING_SERVER_IP_ADDRESS | CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS |
| ID                         | VIRTUAL_SWITCH.ID                      |
| NAME                       | VIRTUAL_SWITCH.NAME                    |
| OPERATIONAL_STATUS         | VIRTUAL_SWITCH.OPERATIONAL_STATUS      |
| SWITCH_MODE                | VIRTUAL_SWITCH.SWITCH_MODE             |
| AD_CAPABLE                 | VIRTUAL_SWITCH.AD_CAPABLE              |
| WWN                        | VIRTUAL_SWITCH.WWN                     |
| ROLE                       | VIRTUAL_SWITCH.ROLE                    |
| FCS_ROLE                   | VIRTUAL_SWITCH.FCS_ROLE                |
| DOMAIN_ID                  | VIRTUAL_SWITCH.DOMAIN_ID               |
| VIRTUAL_FABRIC_ID          | VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID       |
| BASE_SWITCH                | VIRTUAL_SWITCH.BASE_SWITCH             |
| MAX_ZONE_CONFIG_SIZE       | VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE    |
| CREATION_TIME              | VIRTUAL_SWITCH.CREATION_TIME           |
| LAST_UPDATE_TIME           | VIRTUAL_SWITCH.LAST_UPDATE_TIME        |
| USER_NAME                  | VIRTUAL_SWITCH.USER_NAME               |
| PASSWORD                   | VIRTUAL_SWITCH.PASSWORD                |
| MANAGEMENT_STATE           | VIRTUAL_SWITCH.MANAGEMENT_STATE        |
| STATE                      | VIRTUAL_SWITCH.STATE                   |
| STATUS                     | VIRTUAL_SWITCH.STATUS                  |
| STATUS_REASON              | VIRTUAL_SWITCH.STATUS_REASON           |
| FABRIC_IDID_MODE           | VIRTUAL_SWITCH.FABRIC_IDID_MODE        |
| LOGICAL_ID                 | VIRTUAL_SWITCH.LOGICAL_ID              |
| USER_DEFINED_VALUE_1       | VIRTUAL_SWITCH.USER_DEFINED_VALUE_1    |
| USER_DEFINED_VALUE_2       | VIRTUAL_SWITCH.USER_DEFINED_VALUE_2    |
| USER_DEFINED_VALUE_3       | VIRTUAL_SWITCH.USER_DEFINED_VALUE_3    |
| INTEROP_MODE               | VIRTUAL_SWITCH.INTEROP_MODE            |
| CRYPTO_CAPABLE             | VIRTUAL_SWITCH.CRYPTO_CAPABLE          |
| FCR_CAPABLE                | VIRTUAL_SWITCH.FCR_CAPABLE             |
| FCIP_CAPABLE               | VIRTUAL_SWITCH.FCIP_CAPABLE            |
| FABRIC_ID                  | FABRIC_MEMBER.FABRIC_ID                |
| TRUSTED                    | FABRIC_MEMBER.TRUSTED                  |
| MISSING                    | FABRIC_MEMBER.MISSING                  |
| MISSING_TIME               | FABRIC_MEMBER.MISSING_TIME             |

**TABLE 200** SWITCH\_MODEL

| Field       | Definition                                                                                                                   | Format   | Size |
|-------------|------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*         |                                                                                                                              | int      |      |
| SWBD_TYPE   | Switch type number, universally used by all the Management application module implementation.                                | smallint |      |
| SUBTYPE     | Switch subtype. At present no subtypes for existing model records are defined.                                               | smallint |      |
| DESCRIPTION | Model description, such as FC link speed, port count and whether multi-card (director) class switch or other type of switch. | varchar  | 32   |
| MODEL       | Switch model string.                                                                                                         | varchar  | 32   |
| REMARK      | Remarks, such as an internal project name.                                                                                   | varchar  | 64   |

**TABLE 201** PURGED\_SWITCH

| Field                  | Definition              | Format   | Size |
|------------------------|-------------------------|----------|------|
| WWN*                   | WWN of the switch.      | char     | 23   |
| NAME                   | Name of the switch.     | varchar  | 64   |
| VIRTUAL_FABRIC_ID      | Virtual fabric ID.      | smallint |      |
| USER_NAME              | Switch user name.       | varchar  | 64   |
| PASSWORD               | Switch password.        | varchar  | 128  |
| IP_ADDRESS             | IP address.             | varchar  | 128  |
| PORT_NUMBER            | SNMP port number.       | smallint |      |
| RETRY_COUNT            | Retry count.            | smallint |      |
| TIMEOUT                | SNMP time out value.    | smallint |      |
| VERSION                | SNMP version.           | varchar  | 6    |
| READ_COMMUNITY_STRING  | Read community string.  | varchar  | 64   |
| WRITE_COMMUNITY_STRING | Write community string. | varchar  | 64   |
| SNMP_USER_NAME         | SNMP user name.         | varchar  | 128  |
| CONTEXT_NAME           | SNMP context name.      | varchar  | 128  |
| AUTH_PROTOCOL          | SNMP auth protocol.     | varchar  | 16   |
| AUTH_PASSWORD          | snmp auth password      | varchar  | 64   |
| PRIV_PROTOCOL          | snmp priv protocol      | varchar  | 16   |
| PRIV_PASSWORD          | snmp priv password      | varchar  | 64   |

## Switch details

**TABLE 202** CORE\_SWITCH\_DETAILS

| Field                     | Definition                                                                                                                                                            | Format   | Size |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| CORE_SWITCH_ID*           | DB ID.                                                                                                                                                                | int      |      |
| ETHERNET_MASK             | Subnet mask.                                                                                                                                                          | char     | 64   |
| FC_MASK                   | Subnet mask for FC IP.                                                                                                                                                | char     | 64   |
| FC_IP                     | Fibre Channel IP address.                                                                                                                                             | char     | 64   |
| FC_CERTIFICATE            |                                                                                                                                                                       | smallint |      |
| SW_LICENSE_ID             |                                                                                                                                                                       | char     | 23   |
| SUPPLIER_SERIAL_NUMBER    | Serial number of the chassis.                                                                                                                                         | varchar  | 32   |
| PART_NUMBER               | The part number assigned by the organization responsible for producing or manufacturing the PhysicalElement.                                                          | varchar  | 32   |
| CHECK_BEACON              | 1 = beacon is turned on; otherwise, 0.                                                                                                                                | smallint |      |
| TIMEZONE                  | Time zone configured on the switch.                                                                                                                                   | varchar  | 32   |
| FMS_MODE                  | 1 = FICON Management Server mode is enabled on the switch.                                                                                                            | smallint |      |
| MAX_PORT                  | Number of maximum ports physically allowed on the switch.                                                                                                             | smallint |      |
| CHASSIS_SERVICE_TAG       |                                                                                                                                                                       | varchar  | 32   |
| BAY_ID                    |                                                                                                                                                                       | varchar  | 32   |
| TYPE_NUMBER               |                                                                                                                                                                       | varchar  | 32   |
| MODEL_NUMBER              | Switch model number / string.                                                                                                                                         | varchar  | 32   |
| MANUFACTURER              | The name of the organization responsible for producing the chassis. This might be different from the vendor if the product is shipped by an OEM with a private label. | varchar  | 32   |
| PLANT_OF_MANUFACTURE<br>R | Plant where the switch is manufactured.                                                                                                                               | varchar  | 32   |
| SEQUENCE_NUMBER           | Serial number of the switch.                                                                                                                                          | varchar  | 32   |
| TAG                       | An arbitrary string that uniquely identifies the chassis and serves as its physical key. The Tag property contains the WWN of the license switch (LicenseWWN).        | varchar  | 32   |
| DYNAMIC_LOAD_SHARING      |                                                                                                                                                                       | smallint |      |
| PORT_BASED_ROUTING        |                                                                                                                                                                       | smallint |      |
| IN_ORDER_DELIVERY         |                                                                                                                                                                       | smallint |      |
| ACT_CP_PRI_FW_VERSION     | Active CP primary firmware version.                                                                                                                                   | varchar  | 128  |
| ACT_CP_SEC_FW_VERSION     | Active CP secondary firmware version.                                                                                                                                 | varchar  | 128  |

**TABLE 202** CORE\_SWITCH\_DETAILS (Continued)

| Field                  | Definition                                                                        | Format   | Size |
|------------------------|-----------------------------------------------------------------------------------|----------|------|
| STBY_CP_PRI_FW_VERSION | Standby CP primary firmware version.                                              | varchar  | 128  |
| STBY_CP_SEC_FW_VERSION | Standby CP secondary firmware version.                                            | varchar  | 128  |
| TYPE                   | SWBD number as assigned by embedded SW depending upon the switch type / platform. | smallint |      |
| EGM_CAPABLE            | 1 = the switch is EGM-capable.                                                    | smallint |      |
| SUB_TYPE               | SWBD sub type number.                                                             | varchar  | 32   |
| INSISTENT_DID_MODE     | 1 = insistent domain ID mode is enabled on the switch.                            | smallint |      |
| PARTITION              |                                                                                   | smallint |      |

**TABLE 203** CORE\_SWITCH

| Field                | Definition                                                                                                                 | Format    | Size |
|----------------------|----------------------------------------------------------------------------------------------------------------------------|-----------|------|
| ID*                  |                                                                                                                            | int       |      |
| IP_ADDRESS           | IP address of the switch.                                                                                                  | varchar   | 128  |
| WWN                  | Chassis WWN.                                                                                                               | char      | 23   |
| NAME                 | Switch name.                                                                                                               | varchar   | 64   |
| CONTACT              | Any associated contact name, obtained through SNMP.                                                                        | varchar   | 256  |
| LOCATION             | Physical location, obtained through SNMP.                                                                                  | varchar   | 256  |
| DESCRIPTION          | User assigned description, obtained through SNMP.                                                                          | varchar   | 256  |
| TYPE                 | SWBD type number as given by Fabric OS.                                                                                    | smallint  |      |
| MODEL                | Model type of the switch:<br>0 = Unknown<br>1 = Not applicable<br>2 = Fabric OS switch<br>3 = M-EOS switch                 | smallint  |      |
| FIRMWARE_VERSION     | Embedded (Fabric OS or M-EOS) software version.                                                                            | varchar   | 128  |
| VENDOR               | Switch vendor.                                                                                                             | varchar   | 256  |
| MAX_VIRTUAL_SWITCHES | Maximum virtual switches allowed on this physical switch.                                                                  | smallint  |      |
| NUM_VIRTUAL_SWITCHES | Actual number of virtual switches carved out of this physical switch. 0 means it is not operating in Virtual Fabric model. | smallint  |      |
| REACHABLE            | Whether reachable by HTTP.                                                                                                 | smallint  |      |
| UNREACHABLE_TIME     | When the switch became unreachable from HTTP.                                                                              | timestamp |      |
| OPERATIONAL_STATUS   | Operational status as reported by the embedded software.                                                                   | varchar   | 128  |
| CREATION_TIME        | Time when this record is created by the Management application.                                                            | timestamp |      |

**TABLE 203** CORE\_SWITCH (Continued)

| Field                      | Definition                                                                                                                                                                                                          | Format    | Size |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| LAST_SCAN_TIME             |                                                                                                                                                                                                                     | timestamp |      |
| LAST_UPDATE_TIME           | Time when this record was last updated.                                                                                                                                                                             | timestamp |      |
| SYSLOG_REGISTERED          | 1 if the Management application server is registered with the switch to receive Syslog.                                                                                                                             | smallint  |      |
| CALL_HOME_ENABLED          | 1 if "call home" is enabled for this switch.                                                                                                                                                                        | smallint  |      |
| SNMP_REGISTERED            | 1 if the Management application server is registered with the switch to receive SNMP traps.                                                                                                                         | smallint  |      |
| USER_IP_ADDRESS            | User assigned IP address. This is used for M-EOS switches where Fabric OS seed switch fails to get the IP address of the M-EOS switch.                                                                              | varchar   | 128  |
| NIC_PROFILE_ID             | NIC profile of the Management application server host used by this switch to communicate in interactive configuration and other operations. It determines which Management application host IP used by this switch. | int       |      |
| MANAGING_SERVER_IP_ADDRESS | IP address of the server which is currently managing this switch. Used for M-EOS switch only. It does not apply for Fabric OS switches.                                                                             | varchar   | 128  |

**TABLE 204** SWITCH\_DETAILS\_INFO

| Name                        | Source                           |
|-----------------------------|----------------------------------|
| PHYSICAL SWITCH ID          | CORE_SWITCH.ID                   |
| PHYSICAL SWITCH NAME        | CORE_SWITCH.NAME                 |
| IP_ADDRESS                  | CORE_SWITCH.IP_ADDRESS           |
| PHYSICAL SWITCH WWN         | CORE_SWITCH.WWN                  |
| PHYSICAL OPERATIONAL STATUS | CORE_SWITCH.OPERATIONAL_STATUS   |
| TYPE                        | CORE_SWITCH.TYPE                 |
| MAX_VIRTUAL_SWITCHES        | CORE_SWITCH.MAX_VIRTUAL_SWITCHES |
| FIRMWARE_VERSION            | CORE_SWITCH.FIRMWARE_VERSION     |
| VENDOR                      | CORE_SWITCH.VENDOR               |
| REACHABLE                   | CORE_SWITCH.REACHABLE            |
| UNREACHABLE_TIME            | CORE_SWITCH.UNREACHABLE_TIME     |
| CONTACT                     | CORE_SWITCH.CONTACT              |
| LOCATION                    | CORE_SWITCH.LOCATION             |
| DESCRIPTION                 | CORE_SWITCH.DESCRPTION           |
| MODEL                       | CORE_SWITCH.MODEL                |
| SYSLOG_REGISTERED           | CORE_SWITCH.SYSLOG_REGISTERED    |
| SNMP_REGISTERED             | CORE_SWITCH.SNMP_REGISTERED      |
| USER_IP_ADDRESS             | CORE_SWITCH.USER_IP_ADDRESS      |

**TABLE 204** SWITCH\_DETAILS\_INFO

| Name                       | Source                                     |
|----------------------------|--------------------------------------------|
| MANAGING_SERVER_IP_ADDRESS | CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS     |
| ID                         | VIRTUAL_SWITCH.ID                          |
| NAME                       | VIRTUAL_SWITCH.NAME                        |
| OPERATIONAL_STATUS         | VIRTUAL_SWITCH.OPERATIONAL_STATUS          |
| SWITCH_MODE                | VIRTUAL_SWITCH.SWITCH_MODE                 |
| AD_CAPABLE                 | VIRTUAL_SWITCH.AD_CAPABLE                  |
| WWN                        | VIRTUAL_SWITCH.WWN                         |
| ROLE                       | VIRTUAL_SWITCH.ROLE                        |
| FCS_ROLE                   | VIRTUAL_SWITCH.FCS_ROLE                    |
| DOMAIN_ID                  | VIRTUAL_SWITCH.DOMAIN_ID                   |
| VIRTUAL_FABRIC_ID          | VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID           |
| BASE_SWITCH                | VIRTUAL_SWITCH.BASE_SWITCH                 |
| MAX_ZONE_CONFIG_SIZE       | VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE        |
| CREATION_TIME              | VIRTUAL_SWITCH.CREATION_TIME               |
| LAST_UPDATE_TIME           | VIRTUAL_SWITCH.LAST_UPDATE_TIME            |
| USER_NAME                  | VIRTUAL_SWITCH.USER_NAME                   |
| PASSWORD                   | VIRTUAL_SWITCH.PASSWORD                    |
| MANAGEMENT_STATE           | VIRTUAL_SWITCH.MANAGEMENT_STATE            |
| STATE                      | VIRTUAL_SWITCH.STATE                       |
| STATUS                     | VIRTUAL_SWITCH.STATUS                      |
| STATUS_REASON              | VIRTUAL_SWITCH.STATUS_REASON               |
| FABRIC_IDID_MODE           | VIRTUAL_SWITCH.FABRIC_IDID_MODE            |
| LOGICAL_ID                 | VIRTUAL_SWITCH.LOGICAL_ID                  |
| USER_DEFINED_VALUE_1       | VIRTUAL_SWITCH.USER_DEFINED_VALUE_1        |
| USER_DEFINED_VALUE_2       | VIRTUAL_SWITCH.USER_DEFINED_VALUE_2        |
| USER_DEFINED_VALUE_3       | VIRTUAL_SWITCH.USER_DEFINED_VALUE_3        |
| FABRIC_ID                  | FABRIC_MEMBER.FABRIC_ID                    |
| TRUSTED                    | FABRIC_MEMBER.TRUSTED                      |
| MISSING                    | FABRIC_MEMBER.MISSING                      |
| MISSING_TIME               | FABRIC_MEMBER.MISSING_TIME                 |
| ETHERNET_MASK              | CORE_SWITCH_DETAILS.ETHERNET_MASK          |
| FC_MASK                    | CORE_SWITCH_DETAILS.FC_MASK                |
| FC_IP                      | CORE_SWITCH_DETAILS.FC_IP                  |
| FC_CERTIFICATE             | CORE_SWITCH_DETAILS.FC_CERTIFICATE         |
| SW_LICENSE_ID              | CORE_SWITCH_DETAILS.SW_LICENSE_ID          |
| SUPPLIER_SERIAL_NUMBER     | CORE_SWITCH_DETAILS.SUPPLIER_SERIAL_NUMBER |

**TABLE 204** SWITCH\_DETAILS\_INFO

| Name                   | Source                                     |
|------------------------|--------------------------------------------|
| PART_NUMBER            | CORE_SWITCH_DETAILS.PART_NUMBER            |
| CHECK_BEACON           | CORE_SWITCH_DETAILS.CHECK_BEACON           |
| TIMEZONE               | CORE_SWITCH_DETAILS.TIMEZONE               |
| FMS_MODE               | CORE_SWITCH_DETAILS.FMS_MODE               |
| MAX_PORT               | CORE_SWITCH_DETAILS.MAX_PORT               |
| CHASSIS_SERVICE_TAG    | CORE_SWITCH_DETAILS.CHASSIS_SERVICE_TAG    |
| BAY_ID                 | CORE_SWITCH_DETAILS.BAY_ID                 |
| TYPE_NUMBER            | CORE_SWITCH_DETAILS.TYPE_NUMBER            |
| MODEL_NUMBER           | CORE_SWITCH_DETAILS.MODEL_NUMBER           |
| MANUFACTURER           | CORE_SWITCH_DETAILS.MANUFACTURER           |
| PLANT_OF_MANUFACTURER  | CORE_SWITCH_DETAILS.PLANT_OF_MANUFACTURER  |
| SEQUENCE_NUMBER        | CORE_SWITCH_DETAILS.SEQUENCE_NUMBER        |
| TAG                    | CORE_SWITCH_DETAILS.TAG                    |
| DYNAMIC_LOAD_SHARING   | CORE_SWITCH_DETAILS.DYNAMIC_LOAD_SHARING   |
| PORT_BASED_ROUTING     | CORE_SWITCH_DETAILS.PORT_BASED_ROUTING     |
| IN_ORDER_DELIVERY      | CORE_SWITCH_DETAILS.IN_ORDER_DELIVERY      |
| ACT_CP_PRI_FW_VERSION  | CORE_SWITCH_DETAILS.ACT_CP_PRI_FW_VERSION  |
| ACT_CP_SEC_FW_VERSION  | CORE_SWITCH_DETAILS.ACT_CP_SEC_FW_VERSION  |
| STBY_CP_PRI_FW_VERSION | CORE_SWITCH_DETAILS.STBY_CP_PRI_FW_VERSION |
| STBY_CP_SEC_FW_VERSION | CORE_SWITCH_DETAILS.STBY_CP_SEC_FW_VERSION |
| DETAILS TYPE           | CORE_SWITCH_DETAILS.TYPE as DETAILS_TYPE   |
| EGM_CAPABLE            | CORE_SWITCH_DETAILS.EGM_CAPABLE            |
| SUB_TYPE               | CORE_SWITCH_DETAILS.SUB_TYPE               |
| INSISTENT_DID_MODE     | CORE_SWITCH_DETAILS.INSISTENT_DID_MODE     |
| PARTITION              | CORE_SWITCH_DETAILS.PARTITION              |

## Switch port

**TABLE 205** GIGE\_PORT

| Field                    | Definition                                             | Format   | Size |
|--------------------------|--------------------------------------------------------|----------|------|
| ID*                      |                                                        | int      |      |
| SWITCH_PORT_ID           | ID for the GigE Port in SWITCH_PORT.                   | int      |      |
| PORT_NUMBER              | GigE Port Number(0 for ge0 and 1 for ge1).             | int      |      |
| SLOT_NUMBER              | Slot number on which the GigE Port is present.         | int      |      |
| ENABLED                  | Enabled or disabled.                                   | smallint |      |
| SPEED                    | Port speed details.                                    | int      |      |
| MAX_SPEED                | Port maximum speed supported.                          | int      |      |
| MAC_ADDRESS              | MAC Address of that port.                              | varchar  | 64   |
| PORT_NAME                | GigE Port Name.                                        | varchar  | 64   |
| OPERATIONAL_STATUS       | LED status.                                            | int      |      |
| LED_STATE                | LED status.                                            | smallint |      |
| SPEED_LED_STATE          | GigE Port type details.                                | smallint |      |
| PORT_TYPE                | Port type for the GigE Port.                           | varchar  | 64   |
| PERSISTENTLY_DISABLED    | Whether the GigE Port is persistently disabled.        | smallint |      |
| INTERFACE_TYPE           |                                                        | smallint |      |
| CHECKSUM                 |                                                        | varchar  | 16   |
| FCIP_CAPABLE             | 1 = FCIP capable; otherwise, 0.                        | smallint |      |
| ISCSI_CAPABLE            | 1 = ISCSI capable; otherwise, 0.                       | smallint |      |
| INBAND_MANAGEMENT_STATUS | 1 = Inband Management status is enabled; otherwise, 0. | smallint |      |

**TABLE 206** SWITCH\_PORT

| Field             | Definition                                                                                                                            | Format   | Size |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*               |                                                                                                                                       | int      |      |
| VIRTUAL_SWITCH_ID | DB ID of virtual_switch to which this port belongs.                                                                                   | int      |      |
| WWN               | WWN of the port.                                                                                                                      | char     | 23   |
| NAME              | User friendly name of the port.                                                                                                       | char     | 32   |
| SLOT_NUMBER       | Slot number.                                                                                                                          | int      |      |
| PORT_NUMBER       | The logical port number of the user port. There is no assumption of any relation to the physical location of a port within a chassis. | smallint |      |
| USER_PORT_NUMBER  | User port number. Unique port number in a chassis.                                                                                    | smallint |      |
| PORT_ID           | Port ID of this port.                                                                                                                 | varchar  | 8    |
| PORT_INDEX        | Number used for identifying port in zoning.                                                                                           | smallint |      |
| AREA_ID           | Area number the port is assigned to.                                                                                                  | smallint |      |

**TABLE 206** SWITCH\_PORT (Continued)

| Field                 | Definition                                                                         | Format   | Size |
|-----------------------|------------------------------------------------------------------------------------|----------|------|
| MAC_ADDRESS           | MAC address of this port.                                                          | varchar  | 64   |
| PORT_MOD              |                                                                                    | varchar  | 64   |
| TYPE                  | Port type. The specific mode currently enabled for the port.                       | varchar  | 16   |
| FULL_TYPE             | Port type.                                                                         | varchar  | 128  |
| STATUS                | The current status of the switch port.                                             | varchar  | 64   |
| HEALTH                |                                                                                    | varchar  | 16   |
| STATUS_MESSAGE        | Status message if any.                                                             | varchar  | 255  |
| PHYSICAL_PORT         | 1 = it is a physical port<br>0 = it is a virtual port                              | smallint |      |
| LOCKED_PORT_TYPE      | Locked port type.                                                                  | varchar  | 16   |
| CATEGORY              |                                                                                    | smallint |      |
| PROTOCOL              |                                                                                    | varchar  | 16   |
| SPEED                 | Actual speed at which the port is currently operating.                             | varchar  | 64   |
| SPEEDS_SUPPORTED      | Supported speed values.                                                            | varchar  | 32   |
| MAX_PORT_SPEED        | The maximum speed the port is capable of supporting, in bits per second.           | int      |      |
| DESIRED_CREDITS       | How many BB credits are desired for the port.                                      | int      |      |
| BUFFER_ALLOCATED      | How many BB credits are allocated for the port.                                    | int      |      |
| ESTIMATED_DISTANCE    | The estimated physical distance of the connection between ports.                   | int      |      |
| ACTUAL_DISTANCE       | The physical distance of the connection on the port in relation to the other port. | int      |      |
| LONG_DISTANCE_SETTING | Whether long distance enabled.                                                     | int      |      |
| DEGRADED_PORT         | Whether a port is degraded or not.                                                 | varchar  | 16   |
| REMOTE_NODE_WWN       | Node WWN of the attached port.                                                     | varchar  | 255  |
| REMOTE_PORT_WWN       | WWN of the attached port.                                                          | varchar  | 255  |
| LICENSED              | 1 = the port is licensed; otherwise, 0.                                            | smallint |      |
| SWAPPED               | 1 = port is swapped; otherwise, 0.                                                 | smallint |      |
| TRUNKED               | 1 = port is trunked; otherwise, 0.                                                 | smallint |      |
| TRUNK_MASTER          | 1 = the port is trunk master; otherwise, 0.                                        | smallint |      |
| PERSISTENT_DISABLE    | 1 = port is persistently disabled.                                                 | smallint |      |
| FICON_SUPPORTED       | 1 = FICON is supported; otherwise, 0.                                              | smallint |      |
| BLOCKED               | 1 = port is blocked; otherwise, 0.                                                 | smallint |      |
| PROHIBIT_PORT_NUMBERS |                                                                                    | varchar  | 255  |
| PROHIBIT_PORT_COUNT   |                                                                                    | smallint |      |
| NPIV                  | Whether NPIV mode is enabled.                                                      | smallint |      |

**TABLE 206** SWITCH\_PORT (Continued)

| Field                 | Definition                                                                                              | Format   | Size |
|-----------------------|---------------------------------------------------------------------------------------------------------|----------|------|
| NPIV_CAPABLE          | Instance NPIV mode capability:<br>1 = indicates port has NPIV capability<br>2 = NPIV license is enabled | smallint |      |
| NPIV_ENABLED          | Whether NPIV mode is enabled.                                                                           | smallint |      |
| FC_FAST_WRITE_ENABLED | 1 = FC fast write is enabled.                                                                           | smallint |      |
| ISL_RRDY_ENABLED      |                                                                                                         | smallint |      |
| RATE_LIMIT_CAPABLE    |                                                                                                         | smallint |      |
| RATE_LIMITED          |                                                                                                         | smallint |      |
| QOS_CAPABLE           |                                                                                                         | smallint |      |
| TUNNEL_CONFIGURED     |                                                                                                         | smallint |      |
| FCIP_TUNNEL_UP        |                                                                                                         | smallint |      |
| FCR_FABRIC_ID         |                                                                                                         | smallint |      |
| FCR_INTEROP_MODE      |                                                                                                         | smallint |      |
| CALCULATED_STATUS     |                                                                                                         | varchar  | 64   |
| USER_DEFINED_VALUE1   |                                                                                                         | varchar  | 256  |
| USER_DEFINED_VALUE2   |                                                                                                         | varchar  | 256  |
| USER_DEFINED_VALUE3   |                                                                                                         | varchar  | 256  |
| KIND                  |                                                                                                         | varchar  | 32   |
| STATE                 |                                                                                                         | varchar  | 64   |

**TABLE 207** GIGE\_PORT\_INFO

| name                  | Source                          |
|-----------------------|---------------------------------|
| ID                    | GIGE_PORT.ID                    |
| SWITCH_PORT_ID        | GIGE_PORT.SWITCH_PORT_ID        |
| PORT_NUMBER           | GIGE_PORT.PORT_NUMBER           |
| SLOT_NUMBER           | GIGE_PORT.SLOT_NUMBER           |
| ENABLED               | GIGE_PORT.ENABLED               |
| SPEED                 | GIGE_PORT.SPEED                 |
| MAX_SPEED             | GIGE_PORT.MAX_SPEED             |
| MAC_ADDRESS           | GIGE_PORT.MAC_ADDRESS           |
| PORT_NAME             | GIGE_PORT.PORT_NAME             |
| OPERATIONAL_STATUS    | GIGE_PORT.OPERATIONAL_STATUS    |
| LED_STATE             | GIGE_PORT.LED_STATE             |
| SPEED_LED_STATE       | GIGE_PORT.SPEED_LED_STATE       |
| PORT_TYPE             | GIGE_PORT.PORT_TYPE             |
| PERSISTENTLY_DISABLED | GIGE_PORT.PERSISTENTLY_DISABLED |

**TABLE 207** GIGE\_PORT\_INFO (Continued)

| name                     | Source                             |
|--------------------------|------------------------------------|
| INTERFACE_TYPE           | GIGE_PORT.INTERFACE_TYPE           |
| CHECKSUM                 | GIGE_PORT.CHECKSUM                 |
| FCIP_CAPABLE             | GIGE_PORT.FCIP_CAPABLE             |
| ISCSI_CAPABLE            | GIGE_PORT.ISCSI_CAPABLE            |
| INBAND_MANAGEMENT_STATUS | GIGE_PORT.INBAND_MANAGEMENT_STATUS |
| VIRTUAL SWITCHID         | SWITCH_PORT.VIRTUAL_SWITCH_ID      |
| USER PORT NUMBER         | SWITCH_PORT.USER_PORT_NUMBER       |

**TABLE 208** N2F\_PORT\_MAP

| Field             | Definition                                                                                           | Format   | Size |
|-------------------|------------------------------------------------------------------------------------------------------|----------|------|
| ID*               |                                                                                                      | INT      |      |
| VIRTUAL_SWITCH_ID | Virtual switch ID of AG for N to F_port mapping, foreign key to VIRTUAL_SWITCH table.                | INT      |      |
| N_PORT            | Port number of port type N_Port which is being mapped, One N_Port can be mapped to multiple F_ports. | SMALLINT |      |
| F_PORT            | Port number of port type F_Port which is being mapped.                                               | SMALLINT |      |

**TABLE 209** N2F\_PORT\_MAP\_INFO

| Name                 | Source                         |
|----------------------|--------------------------------|
| VIRTUAL SWITCHID     | N2F_PORT_MAP.VIRTUAL_SWITCH_ID |
| N PORT               | N2F_PORT_MAP.N_PORT            |
| F PORT               | N2F_PORT_MAP.F_PORT            |
| EDGE SWITCH PORT WWN | AG_N_PORT.REMOTE_PORT_WWN      |
| AG F PORT WWN        | AG_F_PORT.WWN                  |
| REMOTE NODE WWN      | AG_F_PORT.REMOTE_NODE_WWN      |
| DEVICE PORT WWN      | AG_F_PORT.REMOTE_PORT_WWN      |

**TABLE 210** FPORT\_TRUNK\_GROUP

| Field             | Definition                                                             | Format   | Size |
|-------------------|------------------------------------------------------------------------|----------|------|
| ID*               |                                                                        | INT      |      |
| VIRTUAL_SWITCH_ID | Virtual switch ID where this F_Port Trunk Group is defined.            | INT      |      |
| MASTER_USER_PORT  | User port number for the master port of this trunk.                    | SMALLINT |      |
| WWN               | WWN of the trunk group.                                                | CHAR     | 23   |
| TRUNK_AREA        | User-assigned area number used to group together F_ports of the trunk. | SMALLINT |      |

**TABLE 211** FPORT\_TRUNK\_MEMBER

| Field        | Definition                                 | Format   | Size |
|--------------|--------------------------------------------|----------|------|
| GROUP_ID*    | Foreign key to the PORT_TRUNK_GROUP table. | INT      |      |
| PORT_NUMBER* | Member user port number.                   | SMALLINT |      |
| WWN          | Member port WWN.                           | CHAR     | 23   |

**TABLE 212** VIRTUAL\_SWITCH

| Field                | Definition                                                                         | Format    | Size |
|----------------------|------------------------------------------------------------------------------------|-----------|------|
| ID*                  |                                                                                    | int       |      |
| LOGICAL_ID           | Logical ID of the switch.                                                          | smallint  |      |
| NAME                 | Switch name.                                                                       | varchar   | 64   |
| WWN                  | WWN of the switch.                                                                 | char      | 23   |
| VIRTUAL_FABRIC_ID    | Virtual fabric ID. If VF enabled then will have the VFID; otherwise, it will be -1 | smallint  |      |
| DOMAIN_ID            | Domain ID of the switch.                                                           | smallint  |      |
| BASE_SWITCH          | 1 = this is a base switch; otherwise, 0.                                           | smallint  |      |
| SWITCH_MODE          | 2 = switch is in AG mode; otherwise, 0.                                            | smallint  |      |
| ROLE                 | Role of the switch.                                                                | varchar   | 32   |
| FCS_ROLE             | FCS role of the switch.                                                            | varchar   | 16   |
| AD_CAPABLE           | 1 = switch is AD-capable.                                                          | smallint  |      |
| FABRIC_IDID_MODE     | Fabric IDID mode.                                                                  | smallint  |      |
| OPERATIONAL_STATUS   | Operation status of switch.                                                        | varchar   | 128  |
| MAX_ZONE_CONFIG_SIZE | Maximum size of zone configuration on the switch.                                  | int       |      |
| CREATION_TIME        | Time at which this record was created.                                             | timestamp |      |
| LAST_UPDATE_TIME     | Time when this record was last updated.                                            | timestamp |      |
| USER_NAME            | User name of the switch.                                                           | varchar   | 128  |
| PASSWORD             | Password.                                                                          | varchar   | 128  |
| MANAGEMENT_STATE     | Various states as per manageability software like the Management application.      | int       |      |
| STATE                | State of the switch.                                                               | varchar   | 32   |
| STATUS               | Status of the switch.                                                              | varchar   | 32   |
| STATUS_REASON        | Reason for the status.                                                             | varchar   | 2048 |
| USER_DEFINED_VALUE_1 |                                                                                    | varchar   | 256  |
| USER_DEFINED_VALUE_2 |                                                                                    | varchar   | 256  |
| USER_DEFINED_VALUE_3 |                                                                                    | varchar   | 256  |
| CORE_SWITCH_ID       | Core switch DB ID.                                                                 | int       |      |
| INTEROP_MODE         | Mode in which this switch is operating.                                            | smallint  |      |

**TABLE 212** VIRTUAL\_SWITCH (Continued)

| Field          | Definition                                                                   | Format   | Size |
|----------------|------------------------------------------------------------------------------|----------|------|
| CRYPTO_CAPABLE | 0 = the switch is not crypto-enabled; if capable it will have non-zero value | smallint |      |
| FCR_CAPABLE    | 0 = the switch is not FCR-enabled; if capable it will have non-zero value    | smallint |      |
| FCIP_CAPABLE   | 0 if the switch is not FCIP-enabled; if capable it will have non-zero value  | smallint |      |

## Switch SNMP info

**TABLE 213** VIRTUAL\_SWITCH

| Name                        | Source                      |
|-----------------------------|-----------------------------|
| PHYSICAL SWITCH ID          | PHYSICAL_SWITCH_ID          |
| PHYSICAL SWITCH NAME        | PHYSICAL_SWITCH_NAME        |
| IP ADDRESS                  | IP_ADDRESS                  |
| PHYSICAL SWITCH WWN         | PHYSICAL_SWITCH_WWN         |
| PHYSICAL OPERATIONAL STATUS | PHYSICAL_OPERATIONAL_STATUS |
| TYPE                        | TYPE                        |
| MAX VIRTUAL SWITCHES        | MAX_VIRTUAL_SWITCHES        |
| FIRMWARE VERSION            | FIRMWARE_VERSION            |
| VENDOR                      | VENDOR                      |
| REACHABLE                   | REACHABLE                   |
| UNREACHABLE TIME            | UNREACHABLE_TIME            |
| CONTACT                     | CONTACT                     |
| LOCATION                    | LOCATION                    |
| DESCRIPTION                 | DESCRIPTION                 |
| MODEL                       | MODEL                       |
| ID                          | SWITCH_INFO.ID              |
| NAME                        | SWITCH_INFO.NAME            |
| OPERATIONAL STATUS          | OPERATIONAL_STATUS          |
| SWITCH MAODE                | SWITCH_MODE                 |
| AD CAPABLE                  | AD_CAPABLE                  |
| WWN                         | WWN                         |
| ROLE                        | ROLE                        |
| FCS ROLE                    | FCS_ROLE                    |
| DOMAIN ID                   | DOMAIN_ID                   |
| VIRTUAL FABRIC ID           | VIRTUAL_FABRIC_ID           |

**TABLE 213** VIRTUAL\_SWITCH

| Name                        | Source                                  |
|-----------------------------|-----------------------------------------|
| BASE SWITCH                 | BASE_SWITCH                             |
| MAX ZONE CONFIG SIZE        | MAX_ZONE_CONFIG_SIZE                    |
| CREATION TIME               | CREATION_TIME                           |
| LAST UPDATE TIME            | LAST_UPDATE_TIME                        |
| USER NAME                   | SWITCH_INFO.USER_NAME                   |
| PASSWORD                    | PASSWORD                                |
| MANAGEMENT STATE            | MANAGEMENT_STATE                        |
| STATE                       | STATE                                   |
| STATUS                      | STATUS                                  |
| STATUS REASON               | STATUS_REASON                           |
| USER DEFINED VALUE1         | USER_DEFINED_VALUE_1                    |
| USER DEFINED VALUE2         | USER_DEFINED_VALUE_2                    |
| USER DEFINED VALUE3         | USER_DEFINED_VALUE_3                    |
| FABRIC ID                   | FABRIC_ID                               |
| TRUSTED                     | TRUSTED                                 |
| MISSING                     | MISSING                                 |
| MISSING TIME                | MISSING_TIME                            |
| SNMP PORT NUMBER            | SNMP_CREDENTIALS.PORT_NUMBER            |
| SNMP RETRY COUNT            | SNMP_CREDENTIALS.RETRY_COUNT            |
| SNMP TIMEOUT                | SNMP_CREDENTIALS.TIMEOUT                |
| SNMP VERSION                | SNMP_CREDENTIALS.VERSION                |
| SNMP READ COMMUNITY STRING  | SNMP_CREDENTIALS.READ_COMMUNITY_STRING  |
| SNMP WRITE COMMUNITY STRING | SNMP_CREDENTIALS.WRITE_COMMUNITY_STRING |
| SNMP USER NAME              | SNMP_CREDENTIALS.USER_NAME              |
| SNMP CONTEXT NAME           | SNMP_CREDENTIALS.CONTEXT_NAME           |
| SNMP AUTH PROTOCOL          | SNMP_CREDENTIALS.AUTH_PROTOCOL          |
| SNMP AUTH PASSWORD          | SNMP_CREDENTIALS.AUTH_PASSWORD          |
| SNMP PRIV PROTOCOL          | SNMP_CREDENTIALS.PRIV_PROTOCOL          |
| SNMP PRIV PASSWORD          | SNMP_CREDENTIALS.PRIV_PASSWORD          |

## Threshold

**TABLE 214** SWITCH\_THRESHOLD-SETTING

| Field       | Definition                                                    | Format   | Size |
|-------------|---------------------------------------------------------------|----------|------|
| SWITCH_ID*  | References the ID in CORE_SWITCH table.                       | int      |      |
| POLICY_ID*  | References the ID in THRESHOLD_POLICY table.                  | int      |      |
| STATUS      | The status of applied to the switch.                          | smallint |      |
| OVERRIDDEN  | Policy is overridden or not overridden.                       | smallint |      |
| DESCRIPTION | Description about the status of policy applied to the switch. | varchar  | 100  |

**TABLE 215** THRESHOLD\_POLICY

| Field       | Definition                    | Format  | Size |
|-------------|-------------------------------|---------|------|
| ID*         |                               | int     |      |
| NAME        | Name of the policy.           | varchar | 24   |
| TYPE        | Type of the policy.           | varchar | 20   |
| DESCRIPTION | Description about the policy. | varchar | 100  |

**TABLE 216** FABRIC\_THRESHOLD\_SETTING

| Field      | Definition                                  | Format | Size |
|------------|---------------------------------------------|--------|------|
| FABRIC_ID* | References the ID in FABRIC table           | int    |      |
| POLICY_ID* | References the ID in THRESHOLD_POLICY table | int    | 24   |

**TABLE 217** VIRTUAL\_SWITCH

| Field | Definition | Format | Size |
|-------|------------|--------|------|
| ID*   |            | INT    |      |

**TABLE 218** PM\_MEASURE

| Field       | Definition                      | Format  | Size |
|-------------|---------------------------------|---------|------|
| ID*         |                                 | int     |      |
| DESCRIPTION | The description of the measure. | varchar | 64   |
| NAME        | Name of the measure.            | varchar | 32   |

**TABLE 219** THRESHOLD\_MEASURE

| Field         | Definition                                                             | Format | Size |
|---------------|------------------------------------------------------------------------|--------|------|
| MEASURE_ID*   | References the ID In PM_MEASURE table, where all measures are defined. | int    |      |
| HIGH_BOUNDARY | Configured high boundary threshold value for measure ID.               | int    |      |

**TABLE 219** THRESHOLD\_MEASURE (Continued)

| Field        | Definition                                              | Format | Size |
|--------------|---------------------------------------------------------|--------|------|
| LOW_BOUNDARY | Configured low boundary threshold value for measure ID. | int    |      |
| BUFFER_SIZE  | Configured buffer size for measure ID.                  | int    |      |
| POLICY_ID*   | References the ID in THRESHOLD_POLICY table.            | int    |      |

## User Interface

**TABLE 220** AVAILABLE\_FLYOVER\_PROPERTY

| Field             | Definition                                                                                                                                   | Format   | Size |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------|------|
| ID*               |                                                                                                                                              | int      |      |
| NAME              | Name of the available property to be included in the flyover display.                                                                        | varchar  | 40   |
| TYPE              | The flyover property type:<br>0 = Product property<br>1 = Connection property                                                                | smallint |      |
| DEFAULT_SELECTION | AVAILABLE_FLYOVER_PROPERTY<br>DEFAULT_SELECTION<br>1 = default selected product/connection property<br>0 = not included in the default list. | smallint |      |

**TABLE 221** SELECTED\_FLYOVER\_PROPERTY

| Field        | Definition                                                             | Format  | Size |
|--------------|------------------------------------------------------------------------|---------|------|
| PROPERTY_ID* | Refers to Flyover_Property ID from AVAILABLE_FLYOVER_PROPERTY table.   | int     |      |
| USER_NAME*   | The name of the user who selected the property to be shown on flyover. | varchar | 128  |

**TABLE 222** TOOL\_APP

| Field           | Definition                                                 | Format  | Size |
|-----------------|------------------------------------------------------------|---------|------|
| TOOL_MENU_TEXT* | Text to be displayed for the Tool Menu.                    | varchar | 256  |
| TOOL_ID         | A Tool in the TOOL_PATH table where the tools are defined. | int     |      |
| PARAMETERS      | Default path for launching the tool.                       | varchar | 256  |
| KEY_STROKE      | Short cut key stroke to the application.                   | varchar | 30   |

**TABLE 223** TOOL\_PATH

| Field     | Definition        | Format  | Size |
|-----------|-------------------|---------|------|
| ID*       |                   | int     |      |
| TOOL_NAME | Name of the tool. | varchar | 256  |

**TABLE 223** TOOL\_PATH (Continued)

| Field          | Definition                                     | Format  | Size |
|----------------|------------------------------------------------|---------|------|
| PATH           | Path of the tool where installed or available. | varchar | 1057 |
| WORKING_FOLDER | Working folder for that application.           | varchar | 512  |

**TABLE 224** PRODUCT\_APP

| Field        | Definition                                                                                | Format   | Size |
|--------------|-------------------------------------------------------------------------------------------|----------|------|
| ID*          |                                                                                           | int      |      |
| MENU_TEXT    | Name of the product menu.                                                                 | varchar  | 256  |
| PROP1_KEY    | First condition name to be satisfied by a selected product to launch a particular tool.   | varchar  | 256  |
| PROP1_VALUE  | First condition value to be satisfied by a selected product to launch a particular tool.  | varchar  | 256  |
| PROP2_KEY    | Second condition name to be satisfied by a selected product to launch a particular tool.  | varchar  | 256  |
| PROP2_VALUE  | Second condition value to be satisfied by a selected product to launch a particular tool. | varchar  | 256  |
| TOOL_ID      | The tool to be used for launching the application.                                        | int      |      |
| PARAMETERS   | Link to that application.                                                                 | varchar  | 256  |
| IP_SELECTED  | Selected IP Address option.                                                               | smallint |      |
| WWN_SELECTED | Selected WWN option.                                                                      | smallint |      |

## Zoning 1

**TABLE 225** ZONE\_DB

| Field               | Definition                                                 | Format    | Size |
|---------------------|------------------------------------------------------------|-----------|------|
| ID*                 | PK of the owning fabric.                                   | int       |      |
| FABRIC_ID           | Zone DB name for offline Zone DBs.                         | int       |      |
| NAME                | Offline Zone DB (1 = offline).                             | varchar   | 256  |
| OFFLINE             | Created timestamp.                                         | smallint  |      |
| CREATED             | Last modified timestamp.                                   | timestamp |      |
| LAST_MODIFIED       | Last modified timestamp.                                   | timestamp |      |
| LAST_APPLIED        | Last saved to switch timestamp.                            | timestamp |      |
| CREATED_BY          | Created by user name.                                      | varchar   | 128  |
| LAST_MODIFIED_BY    | Last modified by user name.                                | varchar   | 128  |
| LAST_APPLIED_BY     | Last saved to switch user name.                            | varchar   | 128  |
| DEFAULT_ZONE_STATUS | All access or no access when no active zone configuration. | smallint  |      |
| ZONE_TXN_SUPPORTED  | Zoning commands support transaction.                       | smallint  |      |

**TABLE 225** ZONE\_DB (Continued)

| Field               | Definition                         | Format   | Size |
|---------------------|------------------------------------|----------|------|
| MCDATA_DEFAULT_ZONE | McData switch default zoning mode. | smallint |      |
| MCDATA_SAFE_ZONE    | McData switch safe zoning mode.    | smallint |      |
| ZONE_CONFIG_SIZE    | Zone configuration string length.  | int      |      |

**TABLE 226** ZONE\_DB\_USERS

| Field      | Definition                                    | Format  | Size |
|------------|-----------------------------------------------|---------|------|
| ID*        |                                               | int     |      |
| ZONE_DB_ID | PK of the owning zone DB.                     | int     |      |
| USER_NAME  | List of users currently editing this zone DB. | varchar | 128  |

**TABLE 227** LSAN\_ZONE

| Field          | Definition                   | Format  | Size |
|----------------|------------------------------|---------|------|
| ID*            |                              | int     |      |
| BB_FABRIC_ID   | Backbone fabric DB ID.       | int     |      |
| EDGE_FABRIC_ID | FID assigned to edge fabric. | int     |      |
| NAME           | LSAN zone name.              | varchar | 128  |

**TABLE 228** LSAN\_ZONE\_MEMBER

| Field            | Definition                  | Format | Size |
|------------------|-----------------------------|--------|------|
| LSAN_ZONE_ID*    | LSAN_ZONE record reference. | int    |      |
| MEMBER_PORT_WWN* | Zone member WWN.            | char   | 23   |

**TABLE 229** ZONE\_DB\_CONTENT

| Field      | Definition                                                                  | Format       | Size |
|------------|-----------------------------------------------------------------------------|--------------|------|
| ID*        |                                                                             | int          |      |
| ZONE_DB_ID | PK of the owning offline zone DB.                                           | int          |      |
| CONTENT    | Saved online content before offline was saved to switch.                    | long varchar |      |
| TI_CONTENT | TI_CONTENT saved online TI zone content before offline was saved to switch. | long varchar |      |
| DEFINED    |                                                                             | long varchar |      |
| ACTIVE     |                                                                             | long varchar |      |

## Zoning 2

**TABLE 230** ZONE\_ALIAS\_IN\_ZONE

| Field          | Definition            | Format | Size |
|----------------|-----------------------|--------|------|
| ZONE_ALIAS_ID* | PK of the zone alias. | int    |      |
| ZONE_ID*       | PK of the zone.       | int    | 23   |

**TABLE 231** ZONE\_ALIAS

| Field      | Definition                | Format  | Size |
|------------|---------------------------|---------|------|
| ID*        |                           | int     |      |
| ZONE_DB_ID | PK of the owning ZONE_DB. | int     |      |
| NAME       | The zone alias name.      | varchar | 64   |

**TABLE 232** ZONE\_ALIAS\_MEMBER

| Field         | Definition                                    | Format   | Size |
|---------------|-----------------------------------------------|----------|------|
| ID*           |                                               | int      |      |
| TYPE          | Zone alias member type:<br>2 = WWN<br>4 = D,P | smallint |      |
| VALUE         | Member value (D,P or WWN).                    | varchar  | 256  |
| ZONE_ALIAS_ID | PK of the owning zone alias.                  | int      |      |

**TABLE 233** ZONE\_IN-ZONE\_SET

| Field        | Definition                 | Format | Size |
|--------------|----------------------------|--------|------|
| ZONE_SET_ID* | PK of the owning zone set. | INT    |      |
| ZONE_ID*     | PK of the owning zone.     | INT    |      |

**TABLE 234** ZONE

| Field            | Definition                              | Format   | Size |
|------------------|-----------------------------------------|----------|------|
| ID*              |                                         | int      |      |
| ZONE_DB_ID       | PK the owning ZONE_DB.                  | int      |      |
| NAME             | The zone name.                          | varchar  | 64   |
| TYPE             | The zone type.                          | int      |      |
| SUB_TYPE         | The zone subtype.                       | int      |      |
| ACTIVATE         | For TI zones only, zone is activated.   | smallint |      |
| FAILOVER_ENABLED | For TI zones only, failover is enabled. | smallint |      |

**TABLE 235** ZONE\_DB

| Field               | Definition                                                 | Format    | Size |
|---------------------|------------------------------------------------------------|-----------|------|
| ID*                 |                                                            | int       |      |
| FABRIC_ID           | PK of the owning fabric.                                   |           |      |
| NAME                | Zone DB name for offline Zone DBs.                         | varchar   | 256  |
| OFFLINE             | Offline Zone DB (1 = offline).                             | smallint  |      |
| CREATED             | Created timestamp.                                         | timestamp |      |
| LAST_MODIFIED       | Last modified timestamp.                                   | timestamp |      |
| LAST_APPLIED        | Last saved to switch timestamp.                            | timestamp |      |
| CREATED_BY          | Created by user name.                                      | varchar   | 128  |
| LAST_MODIFIED_BY    | Last modified by user name.                                | varchar   | 128  |
| LAST_APPLIED_BY     | Last saved to switch user name.                            | varchar   | 128  |
| DEFAULT_ZONE_STATUS | All access or no access when no active zone configuration. | smallint  |      |
| ZONE_TXN_SUPPORTED  | Zoning commands support transaction.                       | smallint  |      |
| MCDATA_DEFAULT_ZONE | McData switch default zoning mode.                         | smallint  |      |
| MCDATA_SAFE_ZONE    | McData switch safe zoning mode.                            | smallint  |      |
| ZONE_CONFIG_SIZE    | Zone configuration string length.                          | int       |      |

**TABLE 236** ZONE\_SET

| Field      | Definition                                   | Format   | Size |
|------------|----------------------------------------------|----------|------|
| ID*        |                                              | int      |      |
| ZONE_DB_ID | PK of owning zone DB.                        | int      |      |
| NAME       | Zone set name.                               | varchar  | 64   |
| ACTIVE     | 1 = active zone configuration; otherwise, 0. | smallint |      |

**TABLE 237** ZONE\_MEMBER

| Field   | Definition                         | Format   | Size |
|---------|------------------------------------|----------|------|
| ID*     |                                    | int      |      |
| TYPE    | Member type:<br>2 = WWN<br>4 = D,P | smallint |      |
| VALUE   | Member value (D,P or WWN).         | varchar  | 256  |
| ZONE_ID | PK of owning zone.                 | int      |      |

# Index

---

## A

### access

- assigning, 352
- changing, 353
- removing, 354

### access levels

- defined, 717
- features, 717–718
- roles, 717

### accessing

- FTP server folder, 89

### ACK emulation, device level, 400

### activating

- event policies, 265
- LSAN zones, 631
- PDCM configuration, 474
- zone configuration, 620

### active session management, roles and access levels, 717

### active sessions, viewing, 23

### Adaptive Rate Limiting (ARL), 382

### add/delete properties, roles and access levels, 717

### Adding

- C3 discard frames threshold, 329
- state change threshold, 336, 346

### adding, 258

- destination for syslog forwarding, 284
- detached devices to fabric binding, 242
- event policies, 258
- invalid CRCs thresholds, 331
- invalid words thresholds, 332
- ISL offline policies, 259
- ISL protocol thresholds, 335
- link reset thresholds, 334
- link thresholds, 333
- members to LSAN zone
  - LSAN zone
    - adding members, 629
- PM threshold crossed policies, 260
- property labels, 195
- security thresholds, 338
- security violation policies, 261

### storage ports to storage array, 225

### switches to fabric binding, 241

### thresholds, 329

### traffic isolation zone members, 635

### users, 352

### V1 destination, SNMP traps, 279

### V3 destination, SNMP traps, 280

### zone members, 609

### zones, 619

### admin access, assigning, 352, 353

### administrator access, defined, 717

### administrator privileges, 605

### advanced filtering

- setting up, 254, 275

### alerts, zone configuration comparison, 640

### asset polling, configuring, 99

### assigned thresholds

- finding, 348

### assigning

- event filter to a device, 120
- event filters to call home centers, 120
- threshold policies, 313
- thresholds, 339
- users to resource groups, 361

### associating HBAs to servers, 203

### Authentication type

- PAP, CHAP, 159

## B

### backbone fabric, 488

### backup

- changing interval, 65
- configuration repository, 186
- configuring to hard drive, 62
- configuring to network drive, 63
- configuring to writable CD, 61
- data, 59
- disabling, 64
- enabling, 64
- immediate, 66
- management server, 60

- reviewing events, 66
- roles and access levels, 717
- starting, 66
- status, determining, 10
- switch configuration, 186
- viewing status, 65
- broadcast messages
  - defining, 262
- browse access, assigning, 352, 353

## C

- C3 Discard Frames threshold, 326
- call home, 106
  - centers
    - assigning a device, 118
    - assigning event filters, 120
    - disabling, 116
    - editing, 109
      - Brocade International, 109
      - e-mail, 112
      - EMC, 113
      - HP LAN, 114
      - IBM, 109
      - modem, 111
    - enabling, 115
    - enabling support save, 115
    - hiding, 109
    - removing a device, 118
    - removing all devices and filters, 119
    - removing event filters, 121
    - test connection, 116
    - viewing, 108
  - configuring, 106
  - roles and access levels, 717
  - status, determining, 10
  - system requirements, 107
  - viewing status, 117
- call home event filters table
  - removing event filters, 122
- cascaded FICON fabric
  - configuring, 477
- cascaded FICON fabrics, 467
  - merging, 480
- CEE management, roles and access levels, 717
- CEE switch management
  - using Telnet, 464
  - using Web Tools, 463
- certificates
  - storing the public key, 532

- changing
  - database passwords, 22
  - passwords, 22
  - PDCM matrix display, 475
  - port display, 131
  - port label, 131
  - product label, 131
  - user accounts, 353
  - users, 353
  - view options, 134
- changing connection utilization, 317
- CHAP, 159
- CHAP secret
  - setting, 85
- clearing fabric zone database, 643
- clearing port counters, performance, 296
- client authentication audit trail, displaying, 165
- client export port, configuring, 87
- client/server
  - firewall requirements, 14
- CNA
  - product overview, 366
- collapsing groups, 132
- color, changing, 129, 130
- community strings
  - reverting to default, 41
- comparing
  - zone databases, 638
- concepts, FCIP, 376
- configuration
  - FICON CUP, 467
  - PDCM
    - activating, 474
    - deleting, 475
    - PDCM, copying, 471, 473
    - storage encryption privileges, 495
    - storage port mapping, 224
- configuration file
  - searching, 190
  - viewing, 189
- configuration files, saving, 184, 185
- configuration management
  - roles and access levels, 717
- configuration repository
  - backup, 186
- configuration repository management, overview, 183
- Configure menu, 678

- configuring
    - asset polling, 99
    - call home, 106
    - cascaded FICON fabric, 477
    - client export port, 87
    - discovery, 36, 88
    - e-mail notification, 274
    - encrypted storage in a multi-path environment, 549
    - explicit server IP address, 94
    - external FTP server, 91
    - FCIP advanced settings, 396
    - FCIP tunnels, 391
    - FICON emulation, 399
    - FTP server, 89
    - internal FTP server, 90
    - IP configuration, 93
    - IP interfaces, 391
    - IP routes, 391
    - IPSec and IKE policies, 398
    - LDAP server, 161
    - login banner, 86
    - login security, 85
    - LSAN zoning, 628
    - memory allocation, 97
    - NIS authentication, 164
    - PDCM allow/prohibit matrix, 468
    - Radius server, 159
    - security authentication using the GUI, 373
    - server name, 84
    - server port, 100
    - smart cards, 496
    - SNMP credentials, 39
    - software, 87
    - support mode settings, 101
    - Switch authentication, 162
    - traffic isolation zoning, 633
    - UNIX authentication, 164
    - Windows authentication, 163
    - zoning for the SAN, 607
  - configuring zoning, 607
  - connected ports, showing, 215
  - connection utilization
    - changing, 317
    - disabling, 316
    - enabling, 316
    - overview, 315
    - supported on, 315
  - connections
    - status, determining, 10
  - connections between a switch and an LKM key vault, 585
  - connections, changing display of, 129
  - connections, monitoring utilization, 315
  - content
    - broadcast messages, 262
  - copying
    - log entries, 249
    - log entry parts, 249
    - master log, 252
    - master log parts, 252
    - PDCM configuration, 471, 473
    - threshold policies, 313
    - zones, 644
  - copying views, 127
  - creating
    - LSAN zone, 629
      - new members in LSAN zone
        - LSAN zone
          - creating new members, 630
    - resource groups, 358
    - storage array, 224
    - threshold policies, 309
    - traffic isolation zone, 634
    - user roles, 355
    - views, 124
    - zone, 608
    - zone alias, 615
    - zone configuration, 618
    - zone databases, 623
    - zone members by alias, 613
    - zone members by domain,port, 612
    - zone members by WWN, 610
    - zone sets, 618
  - creating, user accounts, 352
  - CUP, FICON, 467
  - customized views, copying, 127
  - customized views, deleting, 126
  - customized views, editing, 125
  - customizing, product list columns, 124, 125
- ## D
- data
    - historical performance, 297
    - real time performance, 293
  - data backup, 59
  - data collection
    - historical performance, 297
    - historical performance graph, 298
    - historical performance graph configuration, 300
  - data restore, 67
  - database fields
    - Sybase and Derby, 719

- database, restoring, 165
- deactivating
  - event policies, 265
- deactivating zone configuration, 622
- default background color, changing, 130
- default community strings, 41
- default desktop color, changing, 130
- default zone (fabrics)
  - disabling, 614
  - enabling, 614
- defining
  - broadcast messages, 262
  - e-mail messages, 264, 265
  - launch script path, 263
- defining, event filter, 119
- delete
  - switch configuration, 190
- deleting
  - end-to-end monitoring pairs, 304
  - event policies, 266
  - fabrics, 41
  - FCIP tunnels, 408
  - historical performance graph, 301
  - offline zone database, 642
  - PDCM configuration, 475
  - property labels, 196
  - reports, 322
  - storage arrays, 226
  - technical support information, 233
  - threshold policies, 314
  - users, 354
  - zone alias, 641
  - zone configuration, 642
  - zones, 641
- deleting firmware files from
  - firmware repository, 199
- deleting servers, 202
- deleting views, 126
- Derby database fields, 719
- destination
  - adding for syslog forwarding, 284
  - editing for SNMP traps, 281
  - editing for syslog forwarding, 285
  - removing for SNMP traps, 281
  - removing for syslog forwarding, 285
- determining users, 351
- device
  - adding names, 79
  - assigning event filters, 120
  - removing name, 80
- device icons, 11
- device properties, 192
  - viewing, 192
- device properties dialog boxes, customizing, 192
- device shortcut menu
  - adding options, 150
  - changing options, 151
  - removing options, 152
- device tips
  - configuring, 73
- device tips, turning on and off, 76
- device tips, viewing, 76
- diagnose and troubleshooting
  - roles and access levels, 717
- diagnostics
  - types of tests, 364
- directory structure overview, backing up, 60
- disabling
  - call home centers, 116
  - default zone for fabrics, 614
  - fabric binding, 241
  - FCIP tunnels, 407, 408
  - historical performance data collection, 298
  - login banner, 86
  - port connectivity view filter, 211
  - ports, 209
  - safe zoning mode, 615
  - syslog forwarding, 286
  - traffic isolation zone, 636
  - traffic isolation zone failover, 637
- disabling backup, 64
- disabling connection utilization, 316
- disabling SNMP informs, 282
- disabling trap forwarding, 281
- Discover menu, 677
- discovering a fabric, 35
- discovery, 35
  - configuring, 36, 88
  - description of, 364
  - in-band, enabling, 36
  - out-of-band, enabling, 36
  - setting up, 36
  - SNMP version, 36
  - state, 48
  - troubleshooting, 49
- discovery setup
  - roles and access levels, 717
- display
  - end nodes, 70
- display, FICON, 68

- displaying
  - event details, 250, 251
  - FCIP performance graphs for Ethernet ports, 409
  - FCIP performance graphs for FC ports, 409
  - firmware repository, 197
  - master log event details, 250, 251
- downloading
  - firmware, 199
- dual network cards, configuration, 96
- duplicate names, fixing, 78
- duplicating
  - event policies, 266
  - ISL offline policies, 267
  - PM threshold crossed policies, 268
  - security violation policies, 269
  - zone alias, 645
  - zone configuration, 645
  - zones, 644
- Dynamic Load Sharing (DLS), 244

## E

- edge fabrics
  - about, 488
- Edit menu, 675
- editing
  - destination for syslog forwarding, 285
  - destination, SNMP traps, 281
  - event policies, 270
  - ISL offline policies, 271
  - PM threshold crossed policies, 272
  - property fields, 196
  - property labels, 195
  - resource groups, 359
  - security violation policies, 273
  - storage array properties, 226
  - threshold policies, 311
  - thresholds, 340
  - user roles, 356
  - views, 125
  - zone alias, 616
- Element Manager, launching
  - launching Element Manager, 143
- e-mail event notification setup
  - roles and access levels, 717
- e-mail filter override, 353, 372
- e-mail messages
  - defining, 264, 265
- e-mail notification
  - configuring, 274
- emailing
  - technical support information, 232
- enable SSL, 100
- enabling
  - call home centers, 115
  - default zone for fabrics, 614
  - fabric binding, 240
  - FCIP tunnels, 407, 408
  - historical performance data collection, 297
  - port connectivity view filter, 211
  - ports, 209
  - safe zoning mode, 615
  - support save for call home centers, 115
  - syslog forwarding, 285
  - traffic isolation zone, 636
  - traffic isolation zone failover, 637
- enabling backup, 64
- enabling connection utilization, 316
- enabling SNMP informs, 282
- enabling trap forwarding, 279
- encryption
  - adding a target, 571
  - adding new LUNs, 572
  - configuration planning for the management application, 502, 523
  - configure dialog box, 494
  - configuring hosts to access encryption targets, 572
  - configuring in a multi-path environment, 549
  - gathering information before using the setup wizard, 502, 523
  - launching the encryption target properties dialog box, 572
  - launching the encryption targets dialog box, 570
  - moving a target to a different encryption engine, 571
  - removing a target, 571
  - selecting mode for LUNs, 557
  - viewing and editing group properties, 578
- encryption engines
  - adding to HA clusters, 584
  - effects of zeroizing, 569
  - recovering from zeroizing, 569
  - removing from HA clusters, 584
  - support for tape pools, 586
  - zeroizing, 569
- encryption group
  - adding a switch using the management application, 536
  - confirming configuration status, 534
  - creating using the encryption setup wizard, 524
  - selecting the key vault type, 526
  - switch connection requirements, 504

- encryption group properties
  - using the restore master key, 569
  - viewing encryption group properties, 578
- encryption group properties dialog box
  - General tab, 579
  - HA Clusters tab, 542, 584
  - Link Keys tab, 584, 585
  - Members tab, 580
  - Tape Pools tab, 585
- encryption properties
  - viewing properties, 574
- encryption switch or group, removing using the management application, 580
- encryption targets
  - adding to virtual targets and virtual initiators within the encryption switch, 544
  - configuring hosts for, 551
  - using the dialog box, 570
  - using the dialog box to add Disk LUNs, 573
- end nodes
  - display, 70
- end-to-end monitoring
  - configuring pair, 302
  - displaying pairs, 303
  - overview, 302
  - refreshing, 304
- end-to-end monitoring pairs
  - deleting, 304
- Ethernet events
  - disabling, 72
  - enabling, 71
- event details
  - displaying, 250, 251
- event filter
  - assigning, 120
  - assigning to a device, 120
  - defining, 119
  - overwriting, 121
  - removing from device, 122
  - searching for, 122
- event filtering, advanced, 254, 275
- event filters table
  - removing event filters, 122
- event logs, 248
  - copying entries, 249
  - copying parts, 249
  - exporting entries, 250
  - viewing, 248
- event management
  - overview, 247
  - roles and access levels, 717
- event notification
  - configuring e-mail notification, 274
  - overview, 309
- event notification, description, 274
- event policies, 258
  - activating, 265
  - broadcast message, 262
  - deactivating, 265
  - deleting, 266
  - description, 257
  - duplicating, 266
  - editing, 270
  - e-mail messages, 264, 265
  - ISL offline policy, 259
  - ISL offline, duplicating, 267
  - ISL offline, editing, 271
  - launch scripts, 263
  - PM threshold crossed policy, 260
  - PM threshold crossed, duplicating, 268
  - PM threshold crossed, editing, 272
  - security violation policy, 261
  - security violation, duplicating, 269
  - security violation, editing, 273
  - viewing events, 273
- event types, 257, 371
- events
  - Ethernet, 71
  - event types, 257, 371
  - filtering, 253, 353, 372
  - monitoring methods, 247
  - policy actions, 258
  - policy types, 257
  - storage, 72
  - viewing, 273
- expanding groups, 132
- explicit server IP address
  - configuring, 94
- export
  - switch configuration, 191
- exporting
  - log entries, 250
  - master log, 253
  - real time performance data, 296, 301
  - reports, 321
  - storage port mapping, 205, 229
  - zone alias, 617
  - zone databases, 627
- Extended Fabrics license, 480
- external FTP server
  - configuring, 91

## F

- fabric binding
  - adding detached devices, 242
  - adding switches, 241
  - disabling, 241
  - enabling, 240
  - overview, 239
  - removing switches, 242
  - roles and access levels, 717
- Fabric OS
  - seed switch version, 53
- Fabric OS feature listing, 29
- fabric tracking
  - roles and access levels, 717
- fabrics
  - deleting, 41
  - discovering, 35
  - IPv6 discovery, 35
  - monitoring, 52
  - status, determining, 10
  - zone database, clearing, 643
- Fastwrite, 388
- fault management
  - roles and access levels, 717
- FC Address
  - for inactive iSCSI devices, 212, 218
- FC routing module, 144
- FC-FC routing
  - about, 488
  - setting up, 489
  - supported switches, 487
- FCIP
  - advanced settings
    - configuring, 396
  - connection properties
    - viewing, 401
  - DSCP, 386
  - Ethernet connection
    - troubleshooting, 414
  - Ethernet port properties
    - viewing, 404
  - Fastwrite, 388
  - FC port properties
    - viewing, 403
  - IPsec implementation, 384
  - L2CoS, 386
  - management
    - roles and access levels, 717
  - performance graphs, Ethernet ports
    - displaying, 409
  - performance graphs, FC ports
    - displaying, 409
  - properties
    - viewing, 402
  - QoS implementation, 386
  - services
    - licensing, 376
  - Tape Pipelining, 388
  - tunneling, 376
  - tunnels
    - configuring, 391
    - deleting, 408
    - disabling, 407, 408
    - enabling, 407, 408
    - modifying, 405
- FCIP configuration
  - advanced settings, 396
  - IP interfaces, 391
  - IP routes, 391
- FCIP configuration, guidelines, 390
- FCIP trunking, 379
- FCoE management, roles and access levels, 717
- FCR configuration, launching, 144
- feature
  - active session management, 717
  - add/delete properties, 717
  - backup, 717
  - call home, 106, 717
  - CEE management, 717
  - configuration management, 717
  - diagnose and troubleshooting, 717
  - discovery setup, 717
  - e-mail event notification setup, 717
  - event management, 717
  - fabric binding, 717
  - fabric tracking, 717
  - fault management, 717
  - FCIP management, 717
  - FCoE management, 717
  - FICON management, 717
  - firmware management, 717
  - high integrity fabric, 717
  - host management, 717
  - license update, 717
  - licensing requirements, 29
  - Logical Switch Configuration, 717
  - LSAN zoning, 717
  - map port to storage, 717

- performance, 717
  - port fencing, 718
  - product administration, 718
  - product maintenance, 718
  - product operation, 718
  - properties edit, 718
  - report, 718
  - routing configuration, 718
  - security, 718
  - servers, 718
  - setup tools, 718
  - software configuration properties, 718
  - storage encryption configuration, 718
  - storage encryption key operations, 718
  - storage encryption security, 718
  - technical support data collection, 718
  - user management, 718
  - view management, 718
  - zoning activation, 718
  - zoning offline, 718
  - zoning online, 718
  - zoning set edit limits, 718
  - feature-to-firmware requirements, 29
  - Fibre Channel over IP, 376
  - FICON
    - cascaded fabrics, 467
    - configurations, 467
    - configuring emulation, 399
    - CUP, 467
    - display
      - resetting, 69
      - setting, 68
  - FICON management
    - roles and access levels, 717
  - filtering
    - events for users, 353, 372
    - master log events, 253
    - port connectivity view results, 210
    - real time performance data, 295
  - finding
    - assigned thresholds, 348
    - users, 362
  - firmware
    - deleting files from repository, 199
    - downloading, 199
    - management, overview, 197
    - overwriting, 200
  - firmware management
    - roles and access levels, 717
  - firmware repository
    - deleting firmware files, 199
    - displaying, 197
    - importing into, 198
  - flyovers
    - configuring, 73
    - turning on and off, 76
    - viewing, 76
  - FSPF link cost calculation when ARL is used, 382
  - FTP
    - overview, 89
    - server
      - accessing the folder, 89
      - configuring, 89
      - testing, 92
- ## G
- generating
    - performance graph, 294
    - performance reports, 323
    - reports, 320
    - zoning reports, 324
  - graphing
    - end-to-end monitor pairs, historical, 303
    - end-to-end monitor pairs, real time, 303
    - historical performance data collection, 298
  - graphs
    - FCIP performance for Ethernet ports, 409
    - FCIP performance for FC ports, 409
  - group background color, changing, 129
  - grouping
    - overview, 132
  - groups
    - collapsing, 132
    - determining, 362
    - expanding, 132
    - finding users in, 362
    - overview, 132
  - groups, changing color, 129
  - groups, icons, 12
  - guidelines
    - FCIP configuration, 390

## H

- HA clusters
  - creating, 541
  - removing engines from, 542
  - requirements for, 541
  - swapping engines in, 543
- HBAs
  - associating to servers, 203
  - unassociating, 204
- HCM
  - features, 364
  - software overview, 364
  - statistics monitoring, 364
- HCM Agent, launching, 145
- Help menu, 682
- high integrity fabric
  - roles and access levels, 717
- high integrity fabric configuration settings, 477
- high integrity fabrics (HIF), requirements, 467
- historical performance data
  - disabling collection, 298
  - enabling collection, 297
  - graphing, 298
  - overview, 297
  - saving graph configuration, 300
- historical performance graph
  - deleting, 301
- host management, roles and access levels, 717
- host server
  - registering as trap recipient, 278
  - registering for syslog forwarding, 284
  - removing as trap recipient, 279
  - removing for syslog forwarding, 284
- http
  - [//www.gemalto.com/readers/index.html](http://www.gemalto.com/readers/index.html), 496

## I

- icons
  - device, 11
  - products, 11
- IFL. See interfabric links
- IKE policies
  - configuring, 398
- immediate technical support information collection, 231
- import
  - switch configuration, 191

- importing
  - firmware files and release notes, 198
  - storage port mapping, 228
  - zone databases, 627
- inactive iSCSI devices, identifying, 212, 218
- in-band discovery, enabling, 36
- insistent domain ID (IDID), 244
- interfabric links (IFLs), 390
- internal FTP server
  - configuring, 90
- Invalid CRCs threshold, 327
- Invalid CRCs thresholds
  - editing, 340, 341
- invalid CRCs thresholds
  - adding, 331
- Invalid words threshold, 327
- invalid words thresholds
  - adding, 332
  - editing, 342, 344, 345
- IP configuration, 93
- IP frames, 376
- IP interfaces, configuring, 391
- IP routes, configuring, 391
- IPsec
  - FCIP, 384
- IPSec policies
  - configuring, 398
- iSCSI devices, identifying inactive, 212, 218
- ISL offline policies
  - adding, 259
  - duplicating, 267
  - editing, 271
- ISL protocol threshold, 328
  - adding, 335

## K

- keep
  - switch configuration, 191
- key vaults
  - connection from switch, 585
  - entering the IP address or host name for, 527, 528, 529, 530, 531

## L

- launch
  - remote client, 17
- launch script path
  - defining, 263
- launch scripts, 263
  - requirements, 263
- launching
  - Server Management Console, 155
  - SMIA Configuration Tool, 169
- launching FCR configuration, 144
- launching HCM Agent, 145
- launching Telnet, 142
- launching Web Tools, 143
- layout, changing, 128
- layout, overview, 127
- LDAP server
  - configuring, 161
- license keys
  - entering, 25
- license update
  - roles and access levels, 717
- licensing, 25
  - FCIP services, 376
- Lifetime Key Manager (LKM)
  - description of, 507
- link keys, creating, 585
- link reset threshold, 327
- link reset thresholds
  - adding, 334
- link threshold, 327
- link thresholds
  - adding, 333
  - editing, 343
- listing
  - zone members, 648
- LKM
  - creating link keys, 585
  - support for high availability (HA), 510, 517
- Load leveling and failover, 380
- log entries
  - copying, 249
  - copying parts, 249
  - exporting, 250
- logging in
  - remote client, 17
  - remote SMIA configuration tool, 171
  - server, 17

- Logical Switch Configuration
  - roles and access levels, 717
- login banner
  - configuring, 86
  - disabling, 86
- login security
  - configuring, 85
- logon conflicts, 620
- logs
  - event, 248
- LSAN zone
  - creating, 629
- LSAN zones
  - activating, 631
- LSAN zoning
  - configuring, 628
  - overview, 628
  - roles and access levels, 717
- LUN
  - choosing to be added to an encryption target container, 556

## M

- Main window
  - master log, 7
  - menu bar, 3
  - minimap, 9
- main window
  - SAN tab, 4
- Management application
  - server and client, 14
- management application
  - main window, 2
  - user interface, 1
- Management application feature listing, 29
- Management application services
  - monitoring and managing, 156
- management server
  - registering as trap recipient, 278
  - registering for syslog forwarding, 283
- managing
  - zone configuration comparison alerts, 640
- map port to storage
  - roles and access levels, 717

- master key
  - active, 559
  - alternate, 559
  - backup, 560
  - create new master key, 560
  - creating a new, 568
  - description of, 559
  - reasons they are disabled, 560
  - restore master key, 560
  - saving to a file, 560
- master log, 7
  - copying, 252
  - copying parts, 252
  - displaying, 250, 251
  - exporting, 253
  - filtering events, 253
- McDATA fabric mode, 615
- membership list, fabric binding
  - adding detached devices, 242
  - adding switches, 241
  - removing switches, 242
- memory allocation
  - configuration, 97
  - configuring asset polling, 99
- menu bar, 3
  - Configure, 678
  - Discover, 677
  - Edit, 675
  - Help, 682
  - Monitor, 680
  - Server, 675
  - Tools, 681
  - View, 675
- M-EOS feature listing, 29
- merging
  - cascaded FICON fabrics, 480
  - zone databases, 624
- metaSAN, 488
- minimap, 9
  - anchoring, 9
  - attaching, 9
  - detaching, 9
  - floating, 9
  - resizing, 9
- modifying
  - FCIP tunnels, 405
- Monitor menu, 680

- monitoring
  - connection utilization, 315
  - end-to-end, 302
  - end-to-end, configuring, 302
  - end-to-end, displaying, 303
- monitoring fabrics, 52
- monitoring pairs
  - deleting, 304
  - refreshing, 304
- monitoring statistics, 364
- multi-path configuration for encrypted storage using the Management application, 549

## N

- names
  - adding to existing device, 79
  - adding to new device, 80
  - editing, 81
  - exporting, 81
  - fixing duplicates, 78
  - importing, 82
  - removing from device, 80
  - searching by, 82
  - setting as non-unique, 77
  - setting as unique, 76
  - viewing, 79
- names, overview, 76
- naming conventions, 605
- NetApp Lifetime Key Manager (LKM), description of, 507
- NetApp LKM key vaults
  - effects of zeroizing, 569
- new device, adding name, 80
- NIS authentication
  - configuring, 164

## O

- objects
  - removing thresholds, 349
- offline ports, display, 218
- offline zone database
  - deleting, 642
- out-of-band discovery
  - setting up, 36
- overwriting
  - firmware, 200
- overwriting, event filter, 121

## P

PAP, 159

passwords

changing, 22

database, changing, 22

PDCM

E\_Ports, 468

PDCM allow/prohibit matrix

configuring, 468

PDCM configuration

activating, 474

copying, 471, 473

deleting, 475

PDCM matrix display

changing, 475

performance

clearing port counters, 296

roles and access levels, 717

performance data

real time, 293

performance graph

generating, 294

saving historical configuration, 300

performance monitoring

overview, 287

performance measures, 288

thresholds, 309

performance reports

generating, 323

physical map

customizing views, 123

default background color, changing, 130

displaying connections, 129

group background color, changing, 129

layout, changing, 128

layout, overview, 127

levels of detail, 135

port display, changing, 131

port label, changing, 131

product label, changing, 131

showing connected ports, 215

viewing port types, 215

viewing ports, 212

zooming in, 134

zooming out, 134

PM threshold crossed policies

adding, 260

duplicating, 268

editing, 272

policy actions, 258

policy triggers, 258

policy types, 257

port binding, FICON, 244

port connection properties, viewing, 216

port connectivity view

disabling filter, 211

enabling filter, 211

filtering results, 210

refreshing, 209

resetting filter, 211

viewing details, 211

port connectivity, viewing, 206

port display, changing, 131

port fencing

roles and access levels, 718

port fencing inheritance

avoiding, 340

port fencing, description, 325

port label, changing, 131

port optics

refreshing, 220

viewing, 219

port properties, 212

port status, determining, 218

port status, viewing, 24

port types, viewing, 215

port-based routing, 244

ports, 206

determining status, 218

disabling, 209

enabling, 209

showing connected, 215

view connectivity, 206

viewing, 212

viewing connection properties, 216

viewing types, 215

primary FCS, 35

printing

reports, 322

priorities, threshold, 326

privileges

user, 699

privileges, administrator, 605

privileges, user, 495

product administration

roles and access levels, 718

product label, changing, 131

Product list, 5

columns, 5

- product list
  - customizing columns, 124, 125
- product maintenance
  - roles and access levels, 718
- product operation
  - roles and access levels, 718
- product overview, 366
- products
  - icons, 11
  - status, determining, 10
- Prohibit Dynamic Connectivity Mask. See PDCM.
- properties
  - FCIP connection, 401
  - FCIP Ethernet port, 404
  - FCIP FC port, 403
  - general FCIP, 402
  - storage array
    - editing, 226
    - viewing, 227
  - storage port
    - viewing, 227
- properties edit
  - roles and access levels, 718
- property fields
  - editing, 196
- property labels
  - adding, 195
  - deleting, 196
  - editing, 195

## Q

- QoS implementation in FCIP, 386
- QoS priorities per FCIP circuit, 383

## R

- Radius server
  - configuring, 159
- RBAC
  - adding user accounts, 352
  - assigning users to resource groups, 361
  - creating resource groups, 358
  - creating user roles, 355
  - deleting user accounts, 354
  - editing resource groups, 359
  - editing user accounts, 353
  - editing user roles, 356

- removing resource groups, 360
- removing user roles, 357
- removing users from resource groups, 362
- resource groups, 358
- roles, 355
- user list, 351
- user privileges, 699
- users, 351
- real time performance, 293
  - exporting data, 296, 301
  - filtering data, 295
  - graph, 294
- real time performance data
  - thresholds, 309
- reassigning
  - storage ports to storage array, 225
- refreshing
  - end-to-end monitoring pairs, 304
  - port optics view, 220
  - zone databases, 624
- refreshing the port connectivity view, 209
- registering
  - host server, 278
  - host server for syslog forwarding, 284
  - management server, 278
  - management server for syslog forwarding, 283
- registration
  - SNMP traps, 278
- remote client
  - launch, 17
  - logging in, 17
- remote SMIA configuration tool
  - logging in, 171
- removing
  - destination for syslog forwarding, 285
  - destination, SNMP traps, 281
  - host server, 279
  - host server for syslog forwarding, 284
  - members from zone, 648
  - objects from zone alias, 617
  - resource groups, 360
  - servers, 202
  - switches from fabric binding, 242
  - thresholds, 349
  - thresholds from individual objects, 349
  - thresholds from table, 350
  - user roles, 357
  - users, 354
  - users from resource groups, 362
  - zone from zone configuration, 649
  - zones from zone configuration, 649

- removing event filters
  - call home centers, 121
  - call home event filters table, 122
  - devices, 122
- renaming
  - zone alias, 617
  - zone configuration, 650
  - zones, 650
- renaming servers, 202
- replacing
  - zone members, 651
- replicate
  - switch configuration, 191, 192
- report
  - roles and access levels, 718
- report types, 319
- reports
  - deleting, 322
  - exporting, 321
  - generating, 320
  - performance, 323
  - printing, 322
  - viewing, 320
  - zoning, 324
- requirements
  - launch scripts, 263
  - port fencing, 325
- resetting
  - port connectivity view filter, 211
- resource groups
  - assigning users, 361
  - creating, 358
  - editing, 359
  - RBAC, 358
  - removing, 360
  - removing users, 362
- restore
  - switch configuration, 188
- restore data, 67
- restore master key wizard, 569
- restoring
  - database, 165
- reviewing
  - backup events, 66
- role based access control. *See* RBAC.
- role-based access control. *See* RBAC
- roles, 717
  - access levels, 717
  - RBAC, 355

- rolling back changes
  - zone databases, 627
- routing configuration
  - roles and access levels, 718

## S

- safe zoning mode
  - disabling, 615
  - enabling, 615
- SAN
  - zoning, 607
- SAN tab, 4
- saving
  - historical performance graph configuration, 300
  - switch configuration files, 184, 185
  - zone databases to switch, 626
- scheduling
  - technical support information collection, 230
- search
  - names, 82
  - WWN, 83
- searching
  - configuration file, 190
  - members in zones, 646
  - Potential Members list, 646
  - zones in zone configuration, 647
  - Zones list, 647
- security
  - configuring, 84
  - roles and access levels, 718
- security authentication
  - configuring using the GUI, 373
- security tab on management application
  - using to back up a master key, 583
  - using to create a master key, 583
  - using to restore a master key, 583
- security threshold, 328
- security thresholds
  - adding, 338
  - editing, 347
- security violation policies
  - adding, 261
  - duplicating, 269
  - editing, 273
- seed switch, 35, 53
  - change requirements, 54
  - changing, 56
  - FCS policy, 36
- sequential devices, 388, 389

- server IP address, explicit, 94
- Server Management Console
  - about, 155
  - launching, 155
- Server menu, 675
- server name
  - configuring, 84
- server name, determining, 10
- server port
  - configuring, 100
  - enable SSL, 100
- server port numbers, changing, 158
- server properties, viewing, 24
- servers
  - associating to HBAs, 203
  - determining name, 10
  - logging in, 17
  - removing, 202
  - renaming, 202
  - roles and access levels, 718
- setting
  - CHAP secret, 85
- setting up
  - advanced filtering, 254, 275
  - discovery, 36
- setup tools, 141
  - adding menu options, 147
  - adding to device shortcut menu, 150
  - changing menu options, 149
  - changing option on device shortcut menu, 151
  - changing server address, 147
  - removing menu options, 149
  - removing option from device shortcut menu, 152
  - roles and access levels, 718
- show routes
  - requirements, 325
- showing levels of detail, physical map, 135
- showing ports
  - connected, 215
  - procedure, 212
- smart cards
  - configuring, 496
  - removing using the management application, 500
  - saving to a file, 500
- SMIA Configuration Tool
  - launching, 169
- SNMP credentials, configuring, 39
- SNMP informs, disabling, 282
- SNMP informs, enabling, 282
- SNMP traps
  - adding V1 destination, 279
  - adding V3 destination, 280
  - editing a destination, 281
  - registering a different host server, 278
  - registering the management server, 278
  - removing a destination, 281
  - removing the host server, 279
  - trap forwarding, disabling, 281
  - trap forwarding, enabling, 279
- SNMP traps, registration and forwarding, 278
- software configuration, 87
- software configuration properties
  - roles and access levels, 718
- start monitoring, 52
- state change threshold, 328
- status
  - backup, 65
  - discovery, 48
- status bar, 10
- stop monitoring, 53
- storage array
  - adding storage ports to, 225
  - creating, 224
  - deleting, 226
  - reassigning storage ports to, 225
  - unassigning storage ports from, 225
- storage array properties
  - editing, 226
  - viewing, 227
- storage encryption
  - configuration privileges, 495
  - configuring, 545
  - confirming the configuration status, 549
  - selecting the encryption engine for configuration, 546
  - selecting the hosts, 547
  - specifying a name for the target container, 547
- storage encryption configuration
  - roles and access levels, 718
- storage encryption key operations
  - roles and access levels, 718
- storage encryption security
  - privileges for, 495
  - roles and access levels, 718
- storage events
  - configuring, 72
- storage port mapping
  - exporting, 205, 229
  - importing, 228
- storage port mapping configuration, description, 224

- storage port properties
  - viewing, 227
- storage ports
  - adding to storage array, 225
  - reassigning to storage array, 225
  - unassigning from storage array, 225
- support mode
  - configuring, 101
- Switch authentication
  - configuring, 162
- switch binding, FICON, 244
- switch configuration
  - backup, 186
  - deleting, 190
  - exporting, 191
  - file, search content, 190
  - file, view content, 189
  - importing, 191
  - keeping past age limit, 191
  - replicating, 191, 192
  - restore, 188
- switch connection control (SCC) policy, 244
- switch encryption configuration
  - confirm configuration using the management application, 538
  - designate switch membership using the management application, 536
  - specify public key certificate filename using the management application, 537
- switch removal, consequences of, 581
- Sybase database fields, 719
- syslog forwarding
  - adding a destination, 284
  - description, 283, 372
  - disabling, 286
  - editing a destination, 285
  - enabling, 285
  - registering host server, 284
  - registering management server, 283
  - removing a destination, 285
  - removing host server, 284

## T

- tab
  - Authentication (SMC), 160, 161, 162, 163, 164, 165
  - Services (SMC), 165
- tab Ports (SMC), 158
- tab Technical Support Information (SMC), 167
- tab, Services (SMC), 156

- table
  - # Brocade events, 698
  - # CONSRV event, 697
  - # thermal event reason codes, 697
  - call home event, 695
  - features, user groups access levels, 717–718
  - privileges and application behavior, 700–716
- tables
  - advanced call home database fields, 720–??
  - capability database fields, 721–722
  - client\_view database fields, 722–724
  - collector database fields, 725–728
  - config database fields, 728–730
  - connected end devices database fields, 730
  - device database fields, 731–738
  - EE-monitor database fields, 738–740
  - encryption container database fields, 769–773
  - encryption device database fields, 763–768
  - event/FM database fields, 740–746
  - fabric database fields, 746–748
  - FC port status database fields, 749–751
  - FCIP database fields, 752–755
  - FCIP tunnel stats database fields, 755–757
  - GigE port stats database fields, 757–759
  - ISL database fields, 759–762
  - license database fields, 762
  - Meta SAN database fields, 774–776
  - network database fields, 776–777
  - others database fields, 777
  - port fencing database fields, 778
  - quartz database fields, 779–781
  - reports database fields, 782
  - role based access control database fields, 782–784
  - SNMP database fields, 785–787
  - stats database fields, 788–??
  - switch database fields, 790–794
  - switch details database fields, 795–799
  - switch port database fields, 800–805
  - switch SNMP info database fields, 805–806
  - threshold database fields, 807–808
  - UI database fields, 808–809
  - zoning 1 database fields, 809–810
  - zoning 2 database fields, 811–??
- Tape Pipelining, 388
- tape pipelining, 389
- tape pools
  - adding, 586
  - description of, 586
  - identifying using a name or a number, 587
  - modifying, 585
  - removing, 585
- tape read and write acceleration, 388

- tape write acceleration, 389
- technical support data collection
  - roles and access levels, 718
- technical support information
  - copying to an external FTP server, 233
  - deleting, 233
  - emailing, 232
  - immediate, 231
- technical support information collection
  - scheduling, 230
- technical support information, capturing, 167
- technical support information, viewing, 232
- Telnet
  - launching session, 142
- testing
  - FTP server, 92
- third-party tools
  - adding, 141
  - adding menu option, 147
  - adding to device shortcut menu, 150
  - changing menu options, 149
  - changing option on device shortcut menu, 151
  - changing server address, 147
  - removing menu options, 149
  - removing option from device shortcut menu, 152
  - starting, 142
- threshold
  - adding, 329
  - adding C3 discard frames, 329
  - adding state change, 336, 346
  - C3 Discard Frames, 326
  - Invalid CRCs, 327
  - Invalid words, 327
  - ISL protocol, 328
  - link, 327
  - link reset, 327
  - security, 328
  - state change, 328
- threshold policies
  - assigning, 313
  - copying, 313
  - creating, 309
  - deleting, 314
  - editing, 311
- threshold priorities, 326
- thresholds, 326
  - assigning, 339
  - editing, 340
  - finding specific, 348
  - overview, 309
  - removing, 349
  - viewing, 348
  - viewing on a specific device, 349
- thresholds table
  - removing thresholds, 350
- TIN/TUP emulation, 400
- tips, turning on and off, 76
- tips, viewing, 76
- tool tips, turning on and off, 76
- tool tips, viewing, 76
- toolbox, 7
- tools
  - adding, 141
  - adding menu options, 147
  - adding to device shortcut menu, 150
  - changing menu options, 149
  - changing option on device shortcut menu, 151
  - changing server address, 147
  - removing menu options, 149
  - removing option from device shortcut menu, 152
- Tools menu, 681
- tooltips
  - configuring, 73
- topolgy
  - viewing ports, 212
- topology
  - changing port display, 131
  - changing port label, 131
  - changing product label, 131
  - customizing views, 123
  - displaying connections, 129
  - group background color, changing, 129
  - showing connected ports, 215
  - viewing port types, 215
- topology, changing layout, 128
- topology, overview, 127
- topology, See also physical map
- total user count, 10
- traffic isolation zone
  - adding members, 635
  - creating, 634
  - disabling, 636
  - disabling failover, 637
  - enabling, 636
  - enabling failover, 637
- traffic isolation zoning, 632
  - configuring, 633
- trap forwarding
  - disabling, 281
  - enabling, 279
- triggers, 258

troubleshooting  
     discovery, 49  
     FCIP Ethernet connections, 414  
 tunnels, configuring, 391

## U

unassigning  
     storage ports from storage array, 225  
 unassociating, HBA to server, 204  
 UNIX authentication  
     configuring, 164  
 user  
     privileges, 699  
 User Administrator, 699  
 user ID, determining, 10  
 user interface, description, 1  
 user list, viewing, 351  
 user management  
     roles and access levels, 718  
 user privileges  
     defined, 495, 699  
     RBAC, 699  
     resource groups, 495, 699  
 user roles  
     creating, 355  
     editing, 356  
     removing, 357  
 users  
     access levels, 717  
     adding, 352  
     assigning to resource groups, 361  
     changing, 353  
     determining permissions, 362  
     disconnecting, 23  
     filtering events for, 353, 372  
     finding in groups, 362  
     privileges, 699  
     RBAC, 351  
     removing, 354  
     removing from resource groups, 362  
     viewing all, 351  
 users, total, 10  
 using from encryption group properties dialog, 569

## V

V1 destination  
     adding, 279  
 V3 destination  
     adding, 280  
 VE\_Ports, 390  
 VEX\_Port, 390  
 view management, 123  
     roles and access levels, 718  
 View menu, 675  
 view options, changing, 134  
 View window  
     product list, 5  
 View window, toolbox, 7  
 viewing  
     call home status, 117  
     configuration file, 189  
     device properties, 192  
     disabling port connectivity filter, 211  
     enabling port connectivity filter, 211  
     event logs, 248  
     events, 273  
     FCIP connection properties, 401  
     FCIP Ethernet port properties, 404  
     FCIP FC port properties, 403  
     filtering port connectivity, 210  
     general FCIP properties, 402  
     offline ports, 218  
     port connectivity, 206  
     port connectivity details, 211  
     port optics, 219  
     port properties, 212  
     port types, 215  
     ports, 212  
     reports, 320  
     restting port connectivity filter, 211  
     storage array properties, 227  
     storage port properties, 227  
     technical support information, 232  
     thresholds, 348  
     thresholds on a specific device, 349  
     users, 351  
     zooming in, 134  
     zooming out, 134  
 viewing ports  
     connection properties, 216

## views

- copying, 127
- creating, 124
- deleting, 126
- editing, 125

## W

Web Tools, launching, 143

## Windows authentication

- configuring, 163

## WWN

- searching by, 83

## Z

## zeroizing

- effects of using on encryption engine, 569

## zone

- adding to configuration, 619
- alias, 615
- creating, 608
- creating LSAN, 629
- removing, 649
- traffic isolation, adding members, 635
- traffic isolation, creating, 634
- traffic isolation, disabling, 636
- traffic isolation, disabling failover, 637
- traffic isolation, enabling, 636
- traffic isolation, enabling failover, 637

## zone alias

- creating, 615
- deleting, 641
- editing, 616
- exporting, 617

zone alias, duplicating, 645

zone alias, removing objects, 617

zone alias, renaming, 617

## zone configuration

- activating, 620
- adding zones, 619
- creating, 618
- deactivating, 622
- deleting, 642
- duplicating, 645
- finding member in Zones list, 647
- removing a zone, 649
- removing zones, 649
- renaming, 650

## zone configuration comparison alerts

- managing, 640

## zone configuration member

- finding in Zones list, 647

## zone database

- automatic checkout, undoing, 643

## zone databases

- comparing, 638
- creating, 623
- exporting, 627
- importing, 627
- merging, 624
- refreshing, 624
- rolling back changes, 627
- saving to switch, 626

## zone members

- adding to zone, 609
- creating in zone by alias, 613
- creating in zone by domain,port, 612
- creating in zone by WWN, 610
- finding in Potential Members list, 646
- finding in zones, 646
- listing, 648
- removing from zone, 648
- replacing, 651

## zone set

- creating, 618
- naming conventions, 605

zone set. See zone configuration

## zones

- deleting, 641
- duplicating, 644
- finding in zone configuration, 647
- removing from zone configuration, 649
- renaming, 650

## zoning

- accessing, 605
- administrator privileges, 605
- configuration overview, 607
- configuring for the SAN, 607
- invalid names, 605
- LSAN, 628
- naming conventions, 605
- offline, 604
- online, 604
- overview, 603
- traffic isolation, 632
- traffic isolation, configuring, 633

## zoning activation

- roles and access levels, 718

## zoning administration, 638

## Index

- zoning configuration
  - overview, 607
- zoning offline
  - roles and access levels, 718
- zoning online
  - roles and access levels, 718
- zoning reports
  - generating, 324
- zoning set edit limits, roles and access levels, 718
- zooming in, 134
- zooming out, 134